532,072

(12)特許協力条約に基づいて公開された国際[redacted]

(19) 世界知的所有権機関
国際事務局

(43) 国際公開日
2004 年5 月6 日 (06.05.2004)

PCT

(10) 国際公開番号
WO 2004/039116 A1

(51) 国際特許分類[7]: H04Q 7/38, H04L 12/56

(21) 国際出願番号: PCT/JP2003/013624

(22) 国際出願日: 2003 年10 月24 日 (24.10.2003)

(25) 国際出願の言語: 日本語

(26) 国際公開の言語: 日本語

(30) 優先権データ:
特願 2002-311910
2002 年10 月25 日 (25.10.2002) JP

(71) 出願人 (米国を除く全ての指定国について): 松下電器産業株式会社 (MATSUSHITA ELECTRIC INDUSTRIAL CO., LTD.) [JP/JP]; 〒571-8501 大阪府 門真市 大字門真 １００６番地 Osaka (JP).

(71) 出願人 および
(72) 発明者: 田中 武志 (TANAKA,Takeshi) [JP/JP]; 〒239-0847 神奈川県 横須賀市 光の丘６−２−４０６ Kanagawa (JP).

(72) 発明者; および
(75) 発明者/出願人 (米国についてのみ): 青山 高久 (AOYAMA,Takahisa) [JP/JP]; 〒233-0007 神奈川県 横浜市 港南区大久保３−４−１−３１６ Kanagawa (JP).

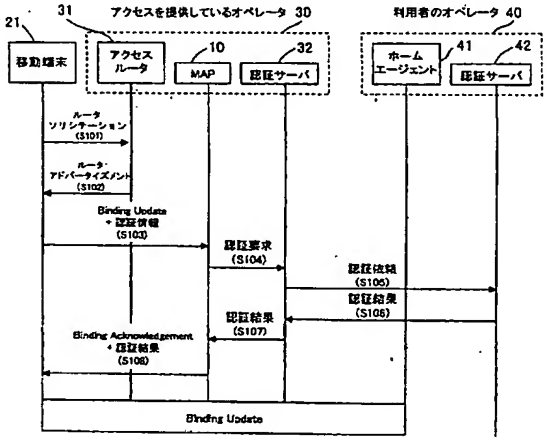
(74) 代理人: 二瓶 正敬 (NIHEI,Masayuki); 〒160-0022 東京都 新宿区 新宿２−８−８ とみん新宿ビル２Ｆ Tokyo (JP).

(81) 指定国 (国内): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR,

[続葉有]

(54) Title: RADIO COMMUNICATION MANAGEMENT METHOD AND RADIO COMMUNICATION MANAGEMENT SERVER

(54) 発明の名称: 無線通信管理方法及び無線通信管理サーバ



21...MOBILE TERMINAL
30...ACCESS PROVIDING OPERATOR
31...ACCESS ROUTER
32...AUTHENTICATION SERVER
40...USER OPERATOR
41...HOME AGENT
42...AUTHENTICATION SERVER
S101...ROUTER SOLICITATION
S102...ROUTER ADVERTISEMENT
S103...BINDING UPDATE AND AUTHENTICATION INFORMATION
S104...AUTHENTICATION REQUEST
S105...AUTHENTICATION ORDER
S106...AUTHENTICATION RESULT
S107...AUTHENTICATION RESULT
S108...BINDING ACKNOWLEDGEMENT AND AUTHENTICATION RESULT

(57) Abstract: The present invention allows a mobile terminal to smoothly perform a handover when changing link connections, and further shortens the time required for changing link connections. When a mobile terminal (21) changes connection links by use of HMIPv6, it transmits authentication information, at the same time as a transmission of information for changing the link connections (Binding Update), to a server (MAP10) that manages link connections of the mobile terminal. When the MAP requests an authentication server (32) for an authentication and acquires an authentication result, then it transmits the authentication result at the same as a transmission of affirmation information of the link connection change (Binding Acknowledgement). Alternatively, the MAP, after receiving the Binding Update and the authentication information from the mobile terminal, may firstly transmit the Binding Acknowledgement and a temporary permission of connection, and then acquire the authentication result to determine whether a formal permission of connection should be given.

(57) 要約: 移動端末がリンク接続を変更する際に、スムーズにハンドオーバを行えるようにするとともに、リンク接続の変更に要する時間を短縮することを目的とし、ＨＭＩＰｖ６を利用して、移動端末２１が接続リンクの変更を行う際、移動端末のリンク接続を管理するサーバ（ＭＡＰ１０）に対して、リンク接続を変更するための情報（Binding Update）と同時に、認証情報の送信を行う。ＭＡＰは、認証サーバ３２に対して認証要求を行って認証結果を取得した場合、リンク接続の変更の確認情報（Binding Acknowledgement）と同時に、認証結果の送信を行う。また、ＭＡＰは、移動端末からBinding Updateと認証情報を受信した後、先にBinding Acknowledgementと仮の接続許可を送り、その後、認証結果を取得して、正式な接続許可を与えるか否かを決定することも可能である。

WO 2004/039116 A1

HU, ID, IL, IN, IS, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) 指定国 (広域): ARIPO 特許 (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), ユーラシア特許 (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), ヨーロッパ特許 (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR), OAPI 特許 (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

添付公開書類:
— 国際調査報告書
— 請求の範囲の補正の期限前の公開であり、補正書受領の際には再公開される。

２文字コード及び他の略語については、定期発行される各*PCT*ガゼットの巻頭に掲載されている「コードと略語のガイダンスノート」を参照。

明　細　書

無線通信管理方法及び無線通信管理サーバ

技術分野

本発明は、移動端末がリンク接続を変更する際に、通信が途切れないように移動端末のアドレスの変更を行う無線通信管理システム及び無線通信管理サーバに関し、特に、ＨＭＩＰｖ６（Hierarchical Mobile IP version 6：階層型モバイルＩＰｖ６）を用いて移動端末のリンク接続を管理する無線通信システムにおける無線通信管理方法及び無線通信管理サーバに関する。

背景技術

利用者が、移動端末（Mobile Terminal）を利用してネットワークと通信を行う場合、アクセスを提供しているオペレータは、移動端末とネットワークとの接続サービスを提供する前に、移動端末がネットワークと接続する権利を有するか否かを判定（認証）する必要がある。この認証処理は、アクセスを提供しているオペレータの施設である中間ノードが、移動端末に対してネットワークとの接続サービスを提供する前に、移動端末からの接続要求に含まれる認証情報（端末ＩＤ及び利用者情報の組合せ）を認証サーバに問い合わせて、認証サーバからの応答に含まれる認証結果に従って、移動端末に対するネットワークとの接続サービスを提供するか否かを判断することにより実現される。なお、必要に応じて、ネットワークを介して、利用者のオペレータの施設に存在する所定の認証サーバに対して認証を依頼することも可能である。本明細書では、このシーケンスを認証シーケンスと呼ぶことにする。

例えば、後述の非特許文献１に記載の技術であるIEEE802.11xを無線ＬＡＮに適用した場合では、移動端末が、ネットワークと接続する際の入り口となるアクセスポイント（Access Point）と接続する際にアクセスポイントに認証情報を送り、アクセスポイントが移動端末の認証サーバに対して認証要求を行うことによって認証処理の実現が可能となっている。

ところで近年、移動端末のワイヤレス化に伴い、移動端末が利用する中間ノードを連続的に切り替えて移動しながら、ネットワークとの継続的な通信を行う場合が増えている。この場合、移動端末にパケットを届けるためには、ネットワーク内のいずれかのノードが、何らかの方法で移動端末の位置を特定する機能を有する必要がある。この移動端末の位置を特定する機能を有するノードは、位置管理サーバと呼ばれ、通常、移動端末の所属する利用者のオペレータに設置される（すなわち、移動端末は、利用者のオペレータの加入者である）。

移動端末がネットワークとの通信を継続しながら、利用する中間ノードを切り替えるシームレスハンドオーバは、通常、ネットワーク内に設置された位置管理サーバに対して、移動端末が位置登録を行うことにより実現可能である。なお、本明細書では、このシーケンスを位置登録シーケンスと呼ぶことにする。

なお、認証シーケンスと位置登録シーケンスとは、シーケンスに係るノードが異なっている。すなわち、認証シーケンスでは、移動端末とネットワークへのアクセスを提供しているドメイン内のサーバとの通信が行われるのに対し、位置登録シーケンスでは、移動端末とネットワーク内の位置管理サーバとの通信が行われる。

移動端末は、認証シーケンスや位置登録シーケンスが完了するまでの間、ネットワークとの通信を行うことができないため、これらのシーケ

ンスはできるだけ短いことが望ましい。このため、後述の非特許文献２に記載されているように、認証シーケンスと位置登録シーケンスとを組み合わせるDiameter Mobile IPv4 Applicationが考えられている。このDiameter Mobile IPv4 Applicationは、IPv4環境下でシームレスハンドオーバを可能とする技術である後述の非特許文献３記載のMobile IPv4シーケンス中に、上記のシーケンスを含めるものである。

図９は、従来の技術に係るDiameter Mobile IPv4 Applicationのシーケンスを示す図である。図９には、利用者がネットワーク５４と接続して通信を行うために利用する移動端末５１、移動端末５１に対してネットワーク５４へのアクセスを提供しているオペレータ５７内のフォーリンエージェント５２及び認証サーバ５３、ネットワーク５４、ネットワーク５４上に存在し、利用者の端末のアドレスを管理する利用者のオペレータ５８内に配置されたホームエージェント５５及び認証サーバ５６が図示されている。

Mobile IPv4機能を搭載した移動端末は、アクセスを提供しているオペレータ５７内（フォーリンネットワーク）に設置された中間ノード（フォーリンエージェント５２）経由で、位置管理サーバ（ホームエージェント５５）に対して位置登録シーケンスを行う。Diameter Mobile IPv4 Applicationでは、Mobile Nodeが位置登録を行う際に、フォーリンエージェント５２に対して送信する位置登録メッセージ（Binding Update）内に、移動端末５１の認証情報が付加され、フォーリンエージェント５２が、アクセスを提供しているオペレータ５７内の認証サーバ５３又は利用者のオペレータ５８内の認証サーバ５６に対して認証要求を行うことにより、認証シーケンスが可能となっている。

一方、移動端末が、ネットワーク上の接続リンクを変更した場合でも、ある特定のアドレス（ＩＰアドレス）を用いて通信することを可能とし、

現在継続中の通信を中断することなくシームレスに接続リンクの変更を可能とするMobileIPv6技術の標準化がIETFのMobile IP Working Groupにおいて進められている。このIPv6環境におけるシームレスハンドオーバをサポートするプロトコルであるMobile IPv6（後述の非特許文献４参照）の位置登録シーケンスは、Mobile IPv4で規定されていたフォーリンエージェント５２のような『アクセスを提供しているオペレータ５７内の中間ノード』を経由せずに行われる。

Mobile IPv6では、基本的に下記の１～３の動作によって、移動端末がアクセスリンク（アクセスネットワーク）に接続中も、ホームアドレス宛てのパケットを受け取ることが可能となる。

１．Care-of Addressの取得

Mobile Nodeは、接続するリンクをアクセスリンクに変更すると、まずそのアクセスリンクより、そのリンク上のＩＰアドレス（ＣｏＡ:Care-of Address）を取得する。これは通常、アクセスルータから定期的にアクセスリンク上の全端末に向けて広告されるルータアドバータイズメント（Router Advertisement）を受信するか、DHCPv6を用いることで実現される。

２．Binding UpdateとBinding Acknowledgement

次に、移動端末は、自分のホームエージェントに対して、その移動端末のホームアドレスとＣｏＡとの組を報告する（Binding Update）。報告を受けたホームエージェントは、その組をテーブルとして保存する。移動端末は接続するリンクを変更する度に、このBinding Updateを行う。ホームエージェントはBinding Updateに対してBinding Acknowledgementを返すが、この過程はBinding Updateにその指示があったときのみ行う。

３．ＩＰトンネリング

この後、ホームエージェントは、移動端末と通信中の端末（

Correspondent Node）からホームリンク（ホームネットワーク）に届いたパケットのうちのテーブル内に登録されたホームアドレス宛てのパケットを、テーブル内に登録されたＣｏＡ宛てのＩＰパケット内のペイロード部分に挿入し、登録されているＣｏＡ宛てのＩＰヘッダを付加して、ＩＰネットワークに転送する（ＩＰトンネリング）。転送されたパケットはＩＰヘッダのＣｏＡに従ってアクセスリンク上に届き、そこから移動端末に配送される。移動端末は、そのパケットのペイロード部分を取得することにより、アクセスリンクに接続しながら、ホームアドレス宛てのパケットを受け取ることができる。

しかしながら、IPv6では、移動端末が接続するリンクを変更した場合、Binding Updateが完了するまでの間は、以前接続していたリンク（接続変更前に接続していたリンク）に、自分のホームアドレス宛てのパケットが届いてしまうことになり、この間は新しい接続リンク先で自分のホームアドレス宛てのパケットを受け取ることが不可能となる。特に、移動端末からホームエージェントまでのネットワーク上の距離（中継するルータ数、中継データリンクの容量などに依存する距離）が離れている場合には、移動端末がホームエージェントにBinding Updateを行うのに必要な時間が長くなり、移動端末が自分のホームアドレス宛てのパケットを受け取れない時間が長くなってしまうという問題点がある。

この問題に対する１つのアプローチとして、後述の非特許文献５に記載されているように、アクセスリンクから比較的近いリンクで構成されたネットワーク上に、新たに移動端末の位置管理を行うサーバを設置し、移動端末がそのネットワーク内でアクセスリンクを変更した場合には、そのサーバに対してCare-of Addressを登録することにより、Binding Update完了までに要する時間を短縮する階層型MobileIPv6（Hierarchical MIPv6：HMIPv6）が、Mobile IP Working Groupで提案され

、現在標準化が行われている。なお、このHMIPv6は、MobileIPv6と共存して動作可能である。

図１０は、従来の技術に係るHMIPv6のシーケンスを示す図である。HMIPv6では、アクセスを提供しているオペレータ６４にＭＡＰ(Mobility Anchor Point) と呼ばれる移動端末６１の比較的狭いリンク内の移動を管理するサーバを設けている。なお、ＭＡＰが管理するリンクはＭＡＰドメインと呼ばれ、ＭＡＰ６２は通常、ＭＡＰドメイン内の上位ネットワークに近い側に設置される。HMIPv6では、次のような動作によって、移動端末６１がＭＡＰドメイン内で移動する場合のBinding過程に必要な時間を短縮することを可能とする。

移動端末６１が、新たにＭＡＰドメインに入るか、又は、異なるＭＡＰドメインに移動して接続リンクを変更した場合、まずアクセスリンクより、そのリンク上のＬＣｏＡ（通常のＣｏＡ：On-Link CoA）を取得し、さらに移動端末６１は、このアクセスリンク上のＭＡＰ６２のアドレスを取得する。移動端末６１は、そのＭＡＰ６２のアドレスから、移動端末６１の別のＣｏＡ（ＲＣｏＡ：Regional CoA）を構成する。そして、移動端末６１は、自端末のＲＣｏＡとＬＣｏＡとの組を、そのＭＡＰ６２に対して登録する（内部位置登録）。ＭＡＰ６２はこの登録に対して、ＯＫの場合には、Binding Acknowledgementを返すとともに、移動端末６１に対して、外部への接続サービスを提供する。また、さらに移動端末６１は、利用者のオペレータ６５のホームエージェント（自端末のホームエージェント）６３に対してＲＣｏＡの登録を行う。（位置登録シーケンス）。

このような位置登録をしておくことによって、移動端末６１が同じＭＡＰドメイン内の異なるリンクに接続を変更した場合には、移動端末６１は、ＭＡＰ６２に対してＬＣｏＡの登録のみを行えばよく、ホームエ

ージェント６３へのＬＣｏＡの登録は不要となる。したがって、移動端末６１がＭＡＰドメイン内を移動する場合であれば、ホームエージェント６３にＣｏＡを登録（Binding Update）し、その確認（Binding Acknowledgement）を受信する一連のBinding過程は省略され、ホームアドレス宛てのパケットを受信できない時間が短縮される。

すなわち、HMIPv6では、移動端末６１が新たにＭＡＰドメイン内のリンクに接続するか、ＭＡＰドメインを変更する場合には、移動端末６１は、ＭＡＰ６２へのＲＣｏＡとＬＣｏＡとの組の登録、及び、ホームエージェント６３へのＲＣｏＡの登録が必要となるが、移動端末６１がＭＡＰドメイン内で接続リンクを変更する場合には、ＭＡＰ６２へのＬＣｏＡの登録のみを行えばよく、ＭＡＰドメイン内での移動時のBinding過程に要する時間を短縮するのに有効である。

非特許文献１

IEEE 802.1 Working Group, "Port-Based Network Access Control", IEEE 802.1x Standard, June 2001.

非特許文献２

Pat R. Calhoun, Tony Johansson, etc., "Diameter Mobile IPv4 Application", Internet Draft, draft-ietf-aaa-diameter-mobileip-13, Oct 2002, Work In Progress.

非特許文献３

Perkins. C, "Mobility Support for IPv4", RFC3220, Jan 2002

非特許文献４

C. Perkins, Jari A., etc., "Mobility Support in IPv6", Internet Draft, draft-ietf-mobileip-ipv6-18, Jun 2002, Work In Progress.

非特許文献５

H. Soliman, C. Castelluccia, etc., "Hierarchical Mobile IPv6

mobility management (HMIPv6)″ Internet Draft,
draft-ietf-mobileip-hmipv6-07, Oct 2002, Work In Progress.

MobileIPv6及びHMIPv6を実際に用いる場合、アクセスを提供しているオペレータと利用者のオペレータとは異なる場合が多く、リンク接続を試みる移動端末に対して認証を行う必要性がある。このためには、移動端末に対して、ＩＰ網の所定のネットワークとの接続サービスを提供する前に、サービスを提供するオペレータが、移動端末から認証情報を取得し、その認証情報を用いて認証処理を行い、認証結果に応じて、接続サービスを提供するか否かを決定する必要がある。

現在、これらの処理を行う条件を満たすものとしては、IEEE802.1xなどのＩＰレベルでの接続を確立するより前に認証を行う技術が挙げられるが、端末の認証の間や、Binding過程（Binding Update及びBinding Acknowledgementのやり取り）が完了するまでの間、移動端末にはＩＰ網からのパケットが届かないことになってしまい、シームレスハンドオーバを実現することは困難となっている。

発明の開示

上記課題に鑑み、本発明は、移動端末がリンク接続を変更するハンドオーバ時に、スムーズにハンドオーバを行えるようにするとともに、リンク接続の変更に要する時間を短縮することを可能とする無線通信管理システム及び無線通信管理サーバを提供することを目的とする。

上記目的を達成するため、本発明では、ＨＭＩＰｖ６を用いて移動端末のリンク接続を管理する無線通信システムにおける無線通信管理方法に関し、移動端末のリンク接続を管理するサーバに対して、移動端末が、リンク接続を変更するための情報と同時に、所望のネットワークにアクセスするための認証に係る情報を送信し、移動端末のリンク接続の変更

に要する時間を短縮するようにしている。

これにより、ＨＭＩＰｖ６において、移動端末がリンク接続を変更するハンドオーバ時に、認証シーケンスと位置登録シーケンスとを同時に実行し、リンク接続の変更に要する時間を短縮することが可能となる。

さらに、本発明では、上記発明に加えて、移動端末が、リンク接続を変更するための情報と、認証に係る情報とを１つの情報として送信し、リンク接続を管理するサーバが、１つの情報から、リンク接続を変更するための情報及び認証に係る情報のそれぞれを取得するようにしている。

これにより、移動端末は、１つの情報の送信を行うだけで、認証要求及び位置登録要求を行うことが可能となる。

さらに、本発明では、上記発明に加えて、リンク接続を管理するサーバが、認証に係る情報を用いた認証処理による認証結果を取得するようにしている。

これにより、認証要求及び位置登録要求を受けたサーバが、認証結果の取得を行うことが可能となる。

さらに、本発明では、上記発明に加えて、リンク接続を管理するサーバが、移動端末の認証を行う認証サーバとの通信を行い、認証結果を取得するようにしている。

これにより、認証要求及び位置登録要求を受けたサーバが、認証サーバに認証依頼を送信し、認証サーバでの認証結果を受信することが可能となる。

さらに、本発明では、上記発明に加えて、移動端末のリンク接続の変更を確認した旨を通知する情報と、認証結果とを１つの情報として、移動端末に送信するようにしている。

これにより、１つの情報の送信によって、認証要求及び位置登録要求を受けたサーバが、移動端末に対してリンク接続の変更の確認情報と認

証結果とを送信できるようになるとともに、認証結果の送信タイミングを定めることが可能となる。

さらに、本発明では、上記発明に加えて、リンク接続を管理するサーバが、移動端末のリンク接続の変更を確認した旨を通知する情報を移動端末に送信し、その後、認証結果を取得できた場合に認証結果を移動端末に送信するようにしている。

これにより、認証要求及び位置登録要求を受けたサーバは、時間がかかると予想される認証結果の取得を待つことなく、まず、リンク接続の変更の確認情報を移動端末に返すことが可能となる。

さらに、本発明では、上記発明に加えて、リンク接続を管理するサーバが、認証結果の取得までの時間を設定し、認証結果の取得までの時間内に認証結果を取得できた場合、次に移動端末からリンク接続を変更するための情報を受信した際に、移動端末のリンク接続の変更を確認した旨を通知する情報と共に、認証結果を移動端末に送信するようにしている。

これにより、認証要求及び位置登録要求を受けたサーバが認証結果を取得した場合に、移動端末に対して認証結果を送信するタイミングを定めることが可能となる。

さらに、本発明では、上記発明に加えて、リンク接続を管理するサーバが、移動端末が所望のネットワークへのアクセスを仮許可する所定の仮許可時間を設定し、移動端末のリンク接続の変更を確認した旨を通知する情報と共に、所定の時間だけ所望のネットワークへのアクセスの許可を通知する情報を移動端末に送信するようにしている。

これにより、認証処理が終わっていない移動端末に対しても接続許可が与えられ、認証処理が完了するのを待つことなく移動端末は、通信を継続することが可能となる。

さらに、本発明では、上記発明に加えて、リンク接続を管理するサーバが、所定の仮許可時間よりも長い時間であって、移動端末が所望のネットワークへのアクセスを許可する所定の許可時間を設定し、認証結果が認証成功であった場合、移動端末のリンク接続の変更を確認した旨を通知する情報と共に、所定の許可時間だけ所望のネットワークへのアクセスの許可を通知する情報を移動端末に送信するようにしている。

これにより、認証に成功した移動端末に対しては、十分に長い有効時間が設定された接続許可を与えることが可能となる。

さらに、本発明では、上記発明に加えて、リンク接続を管理するサーバが、所定の仮許可時間又は所定の許可時間だけ所望のネットワークへのアクセスを許可した移動端末のリンク接続の変更に係る登録を行い、所定の仮許可時間又は所定の許可時間が経過した場合、移動端末のリンク接続の変更に係る登録を削除するようにしている。

これにより、認証が行われている時間だけ移動端末に与えられていた接続許可や、十分に長い時間だけ移動端末に与えられていた接続許可の有効時間が切れた場合、移動端末をリンクから離すことによって、不正なリンク接続が起こらないようにすることが可能となる。

さらに、本発明では、上記発明に加えて、リンク接続を管理するサーバが、認証結果の取得までの時間を設定し、認証結果の取得までの時間内に認証結果を取得できなかった場合、認証結果を認証失敗とするようにしている。

これにより、例えば、認証サーバとの通信が不可能となり、移動端末に係る認証結果が取得できない場合に、移動端末に対して、接続許可を与えないようにすることが可能となる。

さらに、本発明では、上記発明に加えて、リンク接続を管理するサーバが、移動端末に対して所定の接続禁止時間を設定し、移動端末に対し

て認証結果として認証失敗を通知した場合には、認証失敗の通知から所定の接続禁止時間だけ、認証失敗であった移動端末のリンク接続の変更に係る処理及び認証に係る処理を行わないようにしている。

これにより、認証に失敗した移動端末に対して、所定の時間だけ接続禁止の設定を行い、リンク接続の変更要求や認証要求を受けないようにすることで、特に、繰り返し行われる不正なアクセスを防止することが可能となる。

さらに、本発明では、上記発明に加えて、リンク接続を管理するサーバが、移動端末に対して認証結果として認証成功を通知した場合のみ、認証成功であった移動端末のリンク接続の変更に係る登録を行うようにしている。

これにより、認証に成功した移動端末のアドレスのみを登録することが可能となる。

また、上記目的を達成するため、本発明では、移動端末のリンク接続を管理する無線通信システムにおける無線通信管理方法に関し、移動端末のリンク接続を管理するサーバに対して、移動端末が、リンク接続を変更するための情報と同時に、所望のネットワークにアクセスするための認証に係る情報を送信し、リンク接続を管理するサーバが、認証に係る情報を用いた認証処理による認証結果の取得までの時間を設定し、認証結果の取得までの時間内に認証結果を取得できた場合、認証結果を前記移動端末に送信するようにしている。

これにより、認証要求を受けたサーバが認証結果を取得した場合に、移動端末に対して認証結果を送信するタイミングを定めることが可能となる。

さらに、本発明では、上記発明に加えて、リンク接続を管理するサーバが、移動端末が所望のネットワークへのアクセスを仮許可する所定の

仮許可時間を設定し、所定の時間だけ所望のネットワークへのアクセスの許可を通知する情報を移動端末に送信するようにしている。

これにより、認証処理が終わっていない移動端末に対しても接続許可が与えられ、認証処理が完了するのを待つことなく移動端末は、通信を継続することが可能となる。

さらに、本発明では、上記発明に加えて、リンク接続を管理するサーバが、所定の仮許可時間よりも長い時間であって、移動端末が所望のネットワークへのアクセスを許可する所定の許可時間を設定し、認証結果が認証成功であった場合、所定の許可時間だけ所望のネットワークへのアクセスの許可を通知する情報を移動端末に送信するようにしている。

これにより、認証に成功した移動端末に対しては、十分に長い有効時間が設定された接続許可を与えることが可能となる。

さらに、本発明では、上記発明に加えて、所定の仮許可時間又は所定の許可時間が経過した場合、リンク接続を管理するサーバは、移動端末の接続を切断するようにしている。

これにより、認証が行われている時間だけ移動端末に与えられていた接続許可や、十分に長い時間だけ移動端末に与えられていた接続許可の有効時間が切れた場合、移動端末をリンクから離す（ネットワークから切断する）ことによって、不正なリンク接続が起こらないようにすることが可能となる。

また、上記目的を達成するため、本発明では、上記発明に加えて、移動端末のリンク接続を管理する無線通信システムにおける無線通信管理方法に関し、移動端末のリンク接続を管理するサーバに対して、移動端末が、リンク接続を変更するための情報と同時に、所望のネットワークにアクセスするための認証に係る情報を送信し、リンク接続を管理するサーバが、認証に係る情報を用いた認証処理による認証結果の取得まで

の時間を設定し、認証結果の取得までの時間内に認証結果を取得できなかった場合、認証結果を認証失敗とするようにしている。

これにより、例えば、認証サーバとの通信が不可能となり、移動端末に係る認証結果が取得できない場合に、移動端末に対して、接続許可を与えないようにすることが可能となる。

さらに、本発明では、上記発明に加えて、リンク接続を管理するサーバが、移動端末に対して所定の接続禁止時間を設定し、移動端末に対して認証結果として認証失敗を通知した場合には、認証失敗の通知から所定の接続禁止時間だけ、認証失敗であった移動端末に係る処理を行わないようにしている。

これにより、認証に失敗した移動端末に対して、所定の時間だけ接続禁止の設定を行い、リンク接続の変更要求や認証要求を受けないようにすることで、特に、繰り返し行われる不正なアクセスを防止することが可能となる。

さらに、本発明では、上記発明に加えて、リンク接続を管理するサーバが、移動端末に対して認証結果として認証成功を通知した場合のみ、認証成功であった移動端末のリンク接続の変更に係る登録を行うようにしている。

これにより、認証に成功した移動端末のアドレスのみに接続許可を与えることが可能となる。

また、上記目的を達成するため、本発明では、ＨＭＩＰｖ６を用いて移動端末のリンク接続を管理する無線通信管理サーバに関し、移動端末から、リンク接続を変更するための情報と所望のネットワークにアクセスするための認証に係る情報とを１つの情報で受信し、１つの情報から、リンク接続を変更するための情報及び認証に係る情報のそれぞれを取得するよう構成している。

この構成により、移動端末は、１つの情報の送信を行うだけで、認証要求及び位置登録要求を行うことが可能となる。

さらに、本発明では、上記発明に加えて、認証に係る情報を用いた認証処理による認証結果を取得するよう構成している。

この構成により、認証要求及び位置登録要求を受けたサーバが、認証結果の取得を行うことが可能となる。

さらに、本発明では、上記発明に加えて、移動端末の認証を行う認証サーバとの通信を行う手段を有し、認証結果を取得するよう構成している。

この構成により、認証要求及び位置登録要求を受けたサーバが、認証サーバに認証依頼を送信し、認証サーバでの認証結果を受信することが可能となる。

さらに、本発明では、上記発明に加えて、移動端末のリンク接続の変更を確認した旨を通知する情報と認証結果とを１つの情報として、移動端末に送信するよう構成している。

この構成により、１つの情報の送信によって、認証要求及び位置登録要求を受けたサーバが、移動端末に対してリンク接続の変更の確認情報と認証結果とを送信できるようになるとともに、認証結果の送信タイミングを定めることが可能となる。

さらに、本発明では、上記発明に加えて、移動端末のリンク接続の変更を確認した旨を通知する情報を移動端末に送信し、その後、認証結果を取得できた場合に認証結果を移動端末に送信するよう構成している。

この構成により、認証要求及び位置登録要求を受けたサーバは、時間がかかると予想される認証結果の取得を待つことなく、まず、リンク接続の変更の確認情報を移動端末に返すことが可能となる。

さらに、本発明では、上記発明に加えて、認証結果の取得までの時間

を設定する時間設定手段を有し、認証結果の取得までの時間内に認証結果を取得できた場合、次に移動端末からリンク接続を変更するための情報を受信した際に、移動端末のリンク接続の変更を確認した旨を通知する情報と共に、認証結果を移動端末に送信するよう構成している。

この構成により、認証要求及び位置登録要求を受けたサーバが認証結果を取得した場合に、移動端末に対して認証結果を送信するタイミングを定めることが可能となる。

さらに、本発明では、上記発明に加えて、移動端末に対して所望のネットワークへのアクセスを仮許可する所定の仮許可時間を設定する時間設定手段を有し、移動端末のリンク接続の変更を確認した旨を通知する情報と共に、所定の時間だけ所望のネットワークへのアクセスの許可を通知する情報を移動端末に送信するよう構成している

この構成により、認証処理が終わっていない移動端末に対しても接続許可が与えられ、認証処理が完了するのを待つことなく移動端末は、通信を継続することが可能となる。

さらに、本発明では、上記発明に加えて、移動端末に対して、所定の仮許可時間よりも長い時間であって、移動端末が所望のネットワークへのアクセスを許可する所定の許可時間を設定する時間設定手段を有し、認証結果が認証成功であった場合、移動端末のリンク接続の変更を確認した旨を通知する情報と共に、所定の許可時間だけ所望のネットワークへのアクセスの許可を通知する情報を移動端末に送信するよう構成している。

この構成により、認証に成功した移動端末に対しては、十分に長い有効時間が設定された接続許可を与えることが可能となる。

さらに、本発明では、上記発明に加えて、所定の仮許可時間又は所定の許可時間だけ所望のネットワークへのアクセスを許可した移動端末の

リンク接続の変更に係る登録を行う情報登録手段と、所定の仮許可時間又は所定の許可時間が経過した場合、移動端末のリンク接続の変更に係る登録を削除する情報削除手段とを有するよう構成している。

この構成により、認証が行われている時間だけ移動端末に与えられていた接続許可や、十分に長い時間だけ移動端末に与えられていた接続許可の有効時間が切れた場合、移動端末をリンクから離すことによって、不正なリンク接続が起こらないようにすることが可能となる。

さらに、本発明では、上記発明に加えて、認証結果の取得までの時間を設定する時間設定手段と、認証結果の取得までの時間内に認証結果を取得できなかった場合、認証結果を認証失敗とする判定手段とを有するよう構成している。

この構成により、例えば、認証サーバとの通信が不可能となり、移動端末に係る認証結果が取得できない場合に、移動端末に対して、接続許可を与えないようにすることが可能となる。

さらに、本発明では、上記発明に加えて、移動端末に対して所定の接続禁止時間を設定する時間設定手段と、移動端末に対して認証結果として認証失敗を通知した場合には、認証失敗の通知から所定の接続禁止時間だけ、認証失敗であった移動端末のリンク接続の変更に係る処理及び認証に係る処理を行わないよう制御する制御手段とを有するよう構成している。

この構成により、認証に失敗した移動端末に対して、所定の時間だけ接続禁止の設定を行い、リンク接続の変更要求や認証要求を受けないようにすることで、特に、繰り返し行われる不正なアクセスを防止することが可能となる。

さらに、本発明では、上記発明に加えて、移動端末に対して認証結果として認証成功を通知した場合のみ、認証成功であった移動端末のリン

ク接続の変更に係る登録を行うよう制御する制御手段を有するよう構成している。

この構成により、認証に成功した移動端末のアドレスのみを登録することが可能となる。

また、上記目的を達成するため、本発明では、移動端末のリンク接続を管理する無線通信管理サーバに関し、移動端末から、リンク接続を変更するための情報と同時に、所望のネットワークにアクセスするための認証に係る情報を受信する受信手段と、認証に係る情報を用いた認証処理による認証結果の取得までの時間を設定する時間設定手段と、認証結果の取得までの時間内に認証結果を取得できた場合、認証結果を移動端末に送信する送信手段とを有している。

この構成により、認証要求を受けたサーバが認証結果を取得した場合に、移動端末に対して認証結果を送信するタイミングを定めることが可能となる。

さらに、本発明では、上記発明に加えて、移動端末が所望のネットワークへのアクセスを仮許可する所定の仮許可時間を設定する時間設定手段を有し、所定の時間だけ所望のネットワークへのアクセスの許可を通知する情報を移動端末に送信するよう構成している。

この構成により、認証処理が終わっていない移動端末に対しても接続許可が与えられ、認証処理が完了するのを待つことなく移動端末は、通信を継続することが可能となる。

さらに、本発明では、上記発明に加えて、所定の仮許可時間よりも長い時間であって、移動端末が所望のネットワークへのアクセスを許可する所定の許可時間を設定する時間設定手段を有し、認証結果が認証成功であった場合、所定の許可時間だけ所望のネットワークへのアクセスの許可を通知する情報を移動端末に送信するよう構成している。

この構成により、認証に成功した移動端末に対しては、十分に長い有効時間が設定された接続許可を与えることが可能となる。

さらに、本発明では、上記発明に加えて、所定の仮許可時間又は所定の許可時間が経過した場合、移動端末の接続を切断する制御手段を有している。

この構成により、認証が行われている時間だけ移動端末に与えられていた接続許可や、十分に長い時間だけ移動端末に与えられていた接続許可の有効時間が切れた場合、移動端末をリンクから離す（ネットワークから切断する）ことによって、不正なリンク接続が起こらないようにすることが可能となる。

また、上記目的を達成するため、本発明では、移動端末のリンク接続を管理する無線通信システムにおける無線通信管理サーバに関し、移動端末から、リンク接続を変更するための情報と同時に、所望のネットワークにアクセスするための認証に係る情報を受信する受信手段と、リンク接続を管理するサーバが、認証に係る情報を用いた認証処理による認証結果の取得までの時間を設定する時間設定手段と、認証結果の取得までの時間内に認証結果を取得できなかった場合、認証結果を認証失敗として、認証結果を移動端末に送信する送信手段とを有している。

この構成により、例えば、認証サーバとの通信が不可能となり、移動端末に係る認証結果が取得できない場合に、移動端末に対して、接続許可を与えないようにすることが可能となる。

さらに、本発明では、上記発明に加えて、移動端末に対して所定の接続禁止時間を設定する時間設定手段と、移動端末に対して認証結果として認証失敗を通知した場合には、認証失敗の通知から所定の接続禁止時間だけ、認証失敗であった移動端末に係る処理を行わないよう制御する制御手段とを有している。

この構成により、認証に失敗した移動端末に対して、所定の時間だけ接続禁止の設定を行い、リンク接続の変更要求や認証要求を受けないようにすることで、特に、繰り返し行われる不正なアクセスを防止することが可能となる。

さらに、本発明では、上記発明に加えて、移動端末に対して認証結果として認証成功を通知した場合のみ、認証成功であった移動端末のリンク接続の変更に係る登録を行うよう制御する制御手段を有している。

この構成により、認証に成功した移動端末のみを接続許可を与えることが可能となる。

図面の簡単な説明

図１は、本発明の第１の実施の形態におけるＭＡＰの構成を示すブロック図、

図２は、本発明の第１の実施の形態におけるシーケンスを示す図、

図３は、本発明の第２の実施の形態におけるＭＡＰの構成を示すブロック図、

図４は、本発明の第２の実施の形態におけるシーケンスを示す図、

図５は、本発明の第２の実施の形態における移動端末からBinding Updateを受けた際のＭＡＰの処理の詳細を示すフローチャート、

図６は、本発明の第２の実施の形態における状態テーブルの一例を示す模式図、

図７は、本発明の第２の実施の形態における認証サーバ３２から認証結果を受信した場合及び所定の時間が経過した場合のＭＡＰの処理の詳細を示すフローチャート、

図８は、本発明に係る状態テーブルの別の一例を示す模式図、

図９は、従来の技術に係るDiameter Mobile IPv4 Applicationのシー

ケンスを示す図、

図１０は、従来の技術に係るHMIPv6のシーケンスを示す図である。

発明を実施するための最良の形態

以下、図面を参照しながら、本発明の実施の形態について説明する。

（第１の実施の形態）

まず、図面を参照しながら、本発明の第１の実施の形態について説明する。本発明の第１の実施の形態では、ＨＭＩＰｖ６（Hierarchical Mobile IP version 6）の位置登録シーケンス中に認証シーケンスを含めることによって、ハンドオーバに要する時間を短縮し、シームレスな接続サービスを提供することを可能とする技術について説明する。

図１は、本発明の第１の実施の形態におけるＭＡＰの構成を示すブロック図である。図１に示すＭＡＰ（Mobility Anchor Point）１０は、上位ネットワーク２０と接続する上位ネットワーク通信手段１１、下位ネットワーク２５と接続する下位ネットワーク通信手段１２、ＨＭＩＰｖ６を利用したデータ伝送の経路を決定及び制御するＨＭＩＰｖ６経路制御手段１３、認証サーバ３２に対して認証要求の送信及び認証結果の受信を行う認証要求送受信手段１４、データ伝送経路の設定の際に参照されるＨＭＩＰｖ６テーブル１６と認証サーバ３２のアドレス１７とを格納する情報格納手段１５を有している。このうち、本発明の第１の実施の形態に特徴的な構成要素は認証要求送受信手段１４と、情報格納手段１５に格納された認証サーバ３２のアドレス１７であり、上位ネットワーク通信手段１１、下位ネットワーク通信手段１２、ＨＭＩＰｖ６経路制御手段１３は、従来から存在するものを利用することが可能である。なお、ＭＡＰ１０はコンピュータによって実現可能であり、上記の各手段はＣＰＵなどの中央処理手段によって実現可能であるとともに、様々

な情報の参照し、判断・判定処理を行うことも可能である。

図２は、本発明の第１の実施の形態におけるシーケンスを示す図である。図２には、利用者がネットワークと接続して通信を行うために利用する移動端末２１、移動端末２１によるネットワークへのアクセスを提供しているオペレータ３０、利用者のオペレータ４０が図示されている。また、アクセスを提供しているオペレータ３０には、アクセスルータ３１、ＭＡＰ１０、認証サーバ３２が存在し、利用者のオペレータ４０には、ホームエージェント４１、認証サーバ４２が存在する。なお、図２におけるＭＡＰ１０は、図１に示す本発明を実施するためのＭＡＰ１０である。

まず、移動端末２１が新たなリンクに接続した場合、移動端末２１はアクセスルータ３１に対して、ルータアドバータイズメント（Router Advertisement）の送信を促すルータソリシテーション（Router Solicitation）を送信する（ステップＳ１０１）。このルータソリシテーションを受けて、アクセスルータ３１は移動端末２１に対して、ＩＰアドレスなどのルータ情報を含むルータアドバータイズメントを送信する（ステップＳ１０２）。なお、アクセスルータ３１がルータソリシテーションを受けずに、マルチキャストで定期的にルータアドバータイズメントを流すことも可能である。

移動端末２１は、アクセスルータ３１からのルータアドバータイズメントを受けて、接続したリンク上のＩＰアドレス（ＬＣｏＡ：On-link Care-of Address）を取得する。また、移動端末２１の接続したリンクがＭＡＰ１０ドメイン内のリンクである場合、このリンクでのＭＡＰ１０の利用が可能であることがルータアドバータイズメントに示されており、ＨＭＩＰｖ６を搭載した移動端末２１は、ＭＡＰ１０のアドレスを取得することが可能である。そして、このＭＡＰ１０のアドレスから、もう

１つのＣｏＡであるＲＣｏＡ（Regional Care-of Address）を構成する。

次に、ＨＭＩＰｖ６を実装する移動端末２１は、ＭＡＰ１０へのBinding Update（バインディングアップデート：なお、ＢＵと省略することもある）を行うための情報（ＬＣｏＡ）と、端末ＩＤ及び利用者情報を含む認証情報とを、ＭＡＰ１０に対して送信する（ステップＳ１０３）。ＭＡＰ１０は、情報格納手段１５内に格納されている認証サーバ３２のアドレス１７を参照し、認証要求送受信手段１４を用いて、認証サーバ３２に対して認証要求を送信する（ステップＳ１０４）。また、必要ならば、アクセスを提供しているオペレータ３０の認証サーバ３２は、利用者のオペレータ４０の認証サーバ４２に対して認証依頼を送信し（ステップＳ１０５）、認証処理後の応答（認証結果）を受信する（ステップＳ１０６）。そして、認証サーバ３２はＭＡＰ１０に対して、認証結果を返す（ステップＳ１０７）。

なお、上記のステップＳ１０６及びステップＳ１０７の処理が必要でない場合（アクセスを提供しているオペレータ３０の認証サーバ３２において、認証処理が可能な場合）には、アクセスを提供しているオペレータ３０の認証サーバ３２で認証処理を行って、その認証結果をＭＡＰ１０に返すようにする。また、ＭＡＰ１０が、利用者のオペレータ４０の認証サーバ４２と認証依頼及び認証結果のやり取りを直接行うことも可能である。

一方、ＭＡＰ１０は、認証サーバ３２への認証要求の送信と同時にＲＣｏＡ及びＬＣｏＡの登録（Binding Update）を行う。ＭＡＰ１０は、ＲＣｏＡ及びＬＣｏＡの登録が完了し、かつ、認証サーバ３２から認証結果を受けた時点で、Binding Acknowledgement（バインディングアクノレッジメント：なお、ＢＡと省略することもある）と認証結果とを移動端末２１に対して送信する（ステップＳ１０８）。

上記までの動作が終了すると、その後は従来と同様のＨＭＩＰｖ６におけるホームエージェント４１へのBinding Updateが行われる。すなわち、移動端末２１は、ＲＣｏＡをホームエージェント４１に送信して、ホームエージェント４１から登録されたことを示すBinding Acknowledgementを受信する。

以上、説明したように、本発明の第１の実施の形態によれば、シームレスハンドオーバを目的とし、すでに標準化が進められているＨＭＩＰｖ６の位置登録シーケンス中に、認証シーケンスを含めることによって、ＩＰアドレスの移動に係る制御と同時に認証処理を行うことが可能となり、位置登録シーケンスと認証シーケンスが独立に行われていた場合に比べて、ハンドオーバに要する時間が短縮し、移動端末２１に対してシームレスな接続サービスを提供することが可能となる。

（第２の実施の形態）

次に、図面を参照しながら、本発明の第２の実施の形態について説明する。本発明の第２の実施の形態では、ＨＭＩＰｖ６の位置登録シーケンス中に認証シーケンスを含め、さらに、認証処理にかかる時間（認証時間）を考慮して、その認証時間中においても、移動端末２１がネットワークにアクセスできるようにすることによって、ハンドオーバに要する時間を短縮し、シームレスな接続サービスを提供することを可能とする技術について説明する。

これは、特に、アクセスを提供しているオペレータ３０に属するアクセスネットワークと利用者のオペレータ４０に属するホームネットワークとが異なっており、ＭＡＰ１０が認証サーバ３２、４２に対して認証依頼を行ってから認証結果が返ってくるまでの時間が長い場合に有効である。このように認証時間が長くなる理由は、アクセスネットワークとホームネットワークとが離れていることに加え、以下の理由による。

移動端末２１がアクセスネットワークに接続するためには、まず、アクセスネットワークとホームネットワークとが、互いにローミング契約をしている必要があるが、この場合、移動端末２１はアクセスネットワークにとってはローミング端末となるため、アクセスネットワーク内の認証サーバ３２が当該移動端末２１の認証情報を有さないことがある。この場合、通常、アクセスを提供しているオペレータ３０に属する認証サーバ３２（アクセスネットワーク上の認証サーバ３２）が利用者のオペレータ３０に属する認証サーバ４２（ホームネットワーク上の認証サーバ４２）に対して移動端末２１の認証依頼を行う。なお、このような認証情報転送機構は、各オペレータ間のローミング契約や認証サーバ間のプロトコルなどに依存するものである。

図３は、本発明の第２の実施の形態におけるＭＡＰの構成を示すブロック図である。図３に示すＭＡＰ１０は、上位ネットワーク２０と接続する上位ネットワーク通信手段１１、下位ネットワーク２５と接続する下位ネットワーク通信手段１２、ＨＭＩＰｖ６を利用したデータ伝送の経路を決定及び制御するＨＭＩＰｖ６経路制御手段１３、認証サーバ３２に対して認証要求の送信及び認証結果の受信を行う認証要求送受信手段１４、データ伝送経路の設定の際に参照されるＨＭＩＰｖ６テーブル（ＲＣｏＡ／ＬＣｏＡテーブルを含む）１６、認証サーバ３２のアドレス１７、状態テーブル１９を格納する情報格納手段１５、時間管理手段１８を有している。

このうち、本発明の第１の実施の形態に加えて特徴的な構成要素は時間管理手段１８と、情報格納手段１５に格納された状態テーブル１９であり、上位ネットワーク通信手段１１、下位ネットワーク通信手段１２、ＨＭＩＰｖ６経路制御手段１３、認証要求送受信手段１４は、本発明の第１の実施の形態で存在するものを利用することが可能である。なお、

ＭＡＰ１０はコンピュータによって実現可能であり、上記の各手段はＣＰＵなどの中央処理手段によって実現可能であるとともに、様々な情報の参照し、判断・判定処理を行うことも可能である。

時間管理手段１８は、主に、時間を計測する計時機能と、計時結果に従って所定の値を減算（後述の図６に示す状態テーブル１９中の設定値をスタート値とするカウントダウン）し、残り時間が０になったか否かを判定する残り時間判定機能を有している。また、様々な時間情報の設定を行う時間設定手段としての機能も有している。なお、所定の時間が経過したか否かの判定が可能であれば、残り時間判定機能のほかに、所定の時間が経過したか否かを判定する機能、又は、所定の時刻に達したか否かを判定する機能を用いることも可能である。

図４は、本発明の第２の実施の形態におけるシーケンスを示す図である。図４には、図２と同様、移動端末２１、アクセスを提供しているオペレータ３０、利用者のオペレータ４０が図示されており、アクセスを提供しているオペレータ３０には、アクセスルータ３１、ＭＡＰ１０、認証サーバ３２が存在し、利用者のオペレータ４０には、ホームエージェント４１、認証サーバ４２が存在する。なお、図４におけるＭＡＰ１０は、図３に示す本発明を実施するためのＭＡＰ１０である。

第１の実施の形態と同様、移動端末２１が新たなリンクに接続した場合、移動端末２１はアクセスルータに対して、ルータソリシテーションを送信し（ステップＳ２０１）、これを受けて、アクセスルータは移動端末２１に対して、ルータアドバータイズメントを送信する（ステップＳ２０２）。そして、移動端末２１は、アクセスルータからのルータアドバータイズメントを受けて、接続したリンク上のＬＣｏＡとＭＡＰ１０のアドレスとを取得し、ＲＣｏＡを構成する。

次に、ＨＭＩＰｖ６を実装する移動端末２１は、ＭＡＰ１０への

Binding Updateを行うため、ＬＣｏＡと、端末ＩＤ及び利用者情報を含む認証情報とを、ＭＡＰ１０に対して送信する（ステップＳ２０３）。ＭＡＰ１０は、このBinding Updateに関してＲＣｏＡ及びＬＣｏＡの登録を行い、移動端末２１に対して、十分に短い接続の有効時間（仮Binding有効時間Ｔ１）を設定してBinding Acknowledgementを返信する（ステップＳ２０４）。なお、このBinding Acknowledgementは、仮Binding有効時間Ｔ１だけネットワークへの接続許可を与えるものであり、すなわち、このBinding Acknowledgementを受けた移動端末２１は、仮Binding有効時間Ｔ１だけネットワークに接続することが可能となる。

さらに、ＭＡＰ１０は、情報格納手段１５内に格納されている認証サーバ３２のアドレス１７を参照し、認証要求送受信手段１４を用いて、認証サーバ３２に対して認証要求を送信する（ステップＳ２０５）。また、必要ならば、アクセスを提供しているオペレータ３０の認証サーバ３２は、利用者のオペレータ４０の認証サーバ４２に対して認証依頼を送信し（ステップＳ２０６）、認証処理後の応答（認証結果）を受信する（ステップＳ２０７）。そして、認証サーバ３２はＭＡＰ１０に対して、認証結果を返す（ステップＳ２０８）。

なお、第１の実施の形態と同様、上記のステップＳ２０６及びステップＳ２０７の処理が必要でない場合（アクセスを提供しているオペレータ３０の認証サーバ３２において、認証処理が可能な場合）には、アクセスを提供しているオペレータ３０の認証サーバ３２で認証処理を行って、その認証結果をＭＡＰ１０に返すようにする。また、ＭＡＰ１０が、利用者のオペレータ４０の認証サーバ４２と認証依頼及び認証結果のやり取りを直接行うことも可能である。

一方、ＭＡＰ１０は、仮Binding有効時間Ｔ１だけネットワークへの接続が許可された後も、周期的又は仮Binding有効時間Ｔ１に達する直前に

、ＭＡＰ１０へのBinding Updateを行うための情報（ＬＣｏＡ）と、端末ＩＤ及び利用者情報を含む認証情報とを、ＭＡＰ１０に対して送信する（ステップＳ２０９）。

このステップＳ２０９におけるBinding Updateを受けた時点で、ステップＳ２０８における認証サーバ３２からの認証結果の受信が完了している場合には、ＭＡＰ１０は、Binding Acknowledgementと認証結果とを移動端末２１に対して送信する（ステップＳ２１０）。このとき、認証結果が成功を示すものである場合には、ＭＡＰ１０は、移動端末２１に対して、接続許可及び仮Binding有効時間Ｔ１に比べて十分長いBinding有効時間Ｔ２を送信する。このBinding Acknowledgementを受けた移動端末２１は、Binding有効時間Ｔ２だけネットワークに接続することが可能となる。その後は、従来と同様のHMIPｖ６におけるホームエージェント４１へのBinding Updateが行われ、移動端末２１がＲＣｏＡをホームエージェント４１に送信し、ホームエージェント４１から登録完了を示すBinding Acknowledgementを受信する。

一方、図４には不図示だが、ステップＳ２０９におけるBinding Updateを受けた時点で、ステップＳ２０８における認証サーバ３２からの認証結果の受信が完了していない場合（認証結果の受信前に移動端末２１からBinding Updateを再受信した場合）には、ＭＡＰ１０は、再びステップＳ２０４に戻り、移動端末２１に対して仮Binding有効時間Ｔ１だけネットワークへの接続許可を与えるBinding Acknowledgementを送信する。なお、移動端末２１に対して仮Binding有効時間Ｔ１だけネットワークへの接続許可を与えるBinding Acknowledgementを送信する処理は、認証サーバ３２から認証結果を受信するまで繰り返される。

さらに、図４には不図示だが、所定の認証要求有効時間Ｔａが経過しても、認証サーバ３２から認証結果を受信することができなかった場合

（すなわち、ステップＳ２０８の処理が行われなかった場合）には、ＭＡＰ１０は、当該移動端末２１の認証が失敗したとみなして、移動端末２１に対して認証失敗を示す認証結果を送信するとともに、所定の認証要求再開時間Ｔｒの間は接続禁止期間（接続禁止時間）とし、当該移動端末２１からのBinding Updateに対して、接続禁止期間であることを示すBinding Acknowledgementを返すようにする。

また、上記のシーケンスにおいて、移動端末２１からBinding Updateを受けた際のＭＡＰ１０の処理の詳細について説明する。図５は、本発明の第２の実施の形態における移動端末からBinding Updateを受けた際のＭＡＰの処理の詳細を示すフローチャートである。ＭＡＰ１０は、移動端末２１からBinding Updateを受信し（ステップＳ３０１）、状態テーブル１９に当該Binding Updateの送信元の移動端末２１のＬＣｏＡが存在しているか否かを調べる（ステップＳ３０２）。

また、図６は、本発明の第２の実施の形態における状態テーブルの一例を示す模式図である。図６に示されているように、状態テーブル１９には、移動端末２１のＬＣｏＡ、認証結果、認証要求有効時間Ｔａの設定値、認証要求再開時間Ｔｒの設定値、仮Binding時間Ｔ１の設定値、Binding時間Ｔ２の設定値の組み合わせが記録される。なお、認証結果は、この移動端末２１の認証処理における状態や認証結果を含むものであり、例えば、現在認証処理中であることを示す「処理中」、認証に成功したことを示す「認証成功」、認証に失敗したことを示す「認証失敗」、接続が禁止されていることを示す「禁止」などが挙げられる。また、仮Binding時間Ｔ１及び認証要求有効時間Ｔａは認証処理中の状態で付与されるもの、Binding時間Ｔ２は認証成功の状態で付与されるもの、認証要求再開時間Ｔｒは認証失敗の状態で付与されるものである。

この移動端末２１のＬＣｏＡが状態テーブル１９に存在していない場

合には、この移動端末２１のＬＣｏＡを状態テーブル１９に加えて（ステップＳ３０３）、状態テーブル１９中の当該ＬＣｏＡの認証結果を「処理中」にセットする（ステップＳ３０４）。そして、当該ＢＵ中の認証情報（移動端末２１の端末ＩＤや利用者情報）を基にして、この移動端末２１の認証処理を行うよう要求する認証要求を認証サーバ３２に送信し（ステップＳ３０５）、同時に、当該ＬＣｏＡの認証要求有効時間Ｔａをセットし、カウントダウン（減算処理）を開始する（ステップＳ３０６）。

なお、認証要求有効時間Ｔａとして、認証サーバ３２とのやり取りや認証サーバ３２での認証処理にかかる時間より少し長い時間が設定されることが好ましい。また、移動端末２１や認証サーバ３２に係る様々な条件を考慮して、認証要求有効時間Ｔａを移動端末２１毎（ＬＣｏＡ毎）に設定することも可能であり、一律に所定の値に設定することも可能である。

そして、ＲＣｏＡ／ＬＣｏＡテーブルに、この移動端末２１のＲＣｏＡ／ＬＣｏＡの組を追加（登録）し（ステップＳ３０７）、当該ＬＣｏＡの仮Binding時間Ｔ１をセットし、カウントダウン（減算処理）を開始する（ステップＳ３０８）。なお、仮Binding時間Ｔ１として、その時間内では不正なネットワークアクセスが不可能な程度に短い時間が設定されることが好ましい。また、移動端末２１や認証サーバ３２に係る様々な条件を考慮して、仮Binding時間Ｔ１を移動端末２１毎（ＬＣｏＡ毎）に設定することも可能であり、一律に所定の値に設定することも可能である。このようにして設定された接続許可と、接続が許可される有効時間である仮Binding時間Ｔ１とを記載したBinding Acknowledgementを当該移動端末２１に送信し（ステップＳ３０９）、移動端末２１や認証サーバ３２からの応答を受信したり、認証要求有効時間Ｔａや仮Binding

時間Ｔ１のカウントダウンが０になったりする場合まで、待機状態となる。

一方、この移動端末２１のＬＣｏＡが状態テーブル１９に存在している場合には、当該ＬＣｏＡの認証結果が「処理中」であるか否かを調べる（ステップＳ３１０）。当該ＬＣｏＡの認証結果が「処理中」である場合には、Binding Acknowledgement内に「処理中」であることを記載し（ステップＳ３１１）、当該ＬＣｏＡの仮Binding時間Ｔ１をセットし、新たにカウントダウン（減算処理）を開始して（ステップＳ３１２）、新たに設定された接続許可と、接続が許可される有効時間である仮Binding時間Ｔ１とを記載したBinding Acknowledgementを当該移動端末２１に送信する（ステップＳ３１３）。そして、移動端末２１や認証サーバ３２からの応答を受信したり、認証要求有効時間Ｔａや仮Binding時間Ｔ１のカウントダウンが０になったりする場合まで、待機状態となる。

また、当該ＬＣｏＡの認証結果が「処理中」でない場合には、当該ＬＣｏＡの認証結果が「禁止」であるか否かを調べる（ステップＳ３１４）。当該ＬＣｏＡの認証結果が「禁止」である場合には、Binding Acknowledgement内に、接続禁止期間であることを記載して、移動端末２１に送信する（ステップＳ３１５）。

また、当該ＬＣｏＡの認証結果が「禁止」でない場合には、当該ＬＣｏＡの認証結果が「認証成功」であるか否かを調べる（ステップＳ３１６）。当該ＬＣｏＡの認証結果が「認証成功」である場合には、ＲＣｏＡ／ＬＣｏＡテーブルに、この移動端末２１のＲＣｏＡ／ＬＣｏＡの組を追加（登録）し（ステップＳ３１７）、当該ＬＣｏＡのBinding時間Ｔ２をセットし、カウントダウン（減算処理）を開始する（ステップＳ３１８）。なお、Binding時間Ｔ２として、移動端末２１に十分な接続サー

ビスを提供できる程度に長い時間が設定されることが好ましい。また、移動端末２１や認証サーバ３２に係る様々な条件を考慮して、Binding時間Ｔ２を移動端末２１毎(ＬＣｏＡ毎)に設定することも可能であり、一律に所定の値に設定することも可能である。ＭＡＰ１０は、このようにして設定された接続許可と、接続が許可される有効時間であるBinding時間Ｔ２とを記載したBinding Acknowledgementを当該移動端末２１に送信し（ステップＳ３１９）、移動端末２１に対して、Binding時間Ｔ２の接続サービスを提供する。

また、当該ＬＣｏＡの認証結果が「認証成功」でない場合には、当該ＬＣｏＡの認証結果は「認証失敗」であるとみなされ、Binding Acknowledgement内に、認証失敗であることを記載して、移動端末２１に送信する（ステップＳ３２０）。また、所定の時間（認証要求再開時間Ｔｒ）だけの期間、その移動端末２１の認証処理を行わないようにするため、状態テーブル１９中の当該移動端末２１のＬＣｏＡの認証結果を「禁止」にセットし（ステップＳ３２１）、同時に、当該ＬＣｏＡの認証要求再開時間Ｔｒをセットし、カウントダウン（減算処理）を開始する（ステップＳ３２２）。

図５に示すフローチャートでは、ＭＡＰ１０は、所定の処理を終了して待機状態となる。この待機状態では、ＭＡＰ１０は、移動端末２１や認証サーバ３２からの応答の受信を待機する状態、仮Binding時間Ｔ１、Binding時間Ｔ２、認証要求有効時間Ｔａ、認証要求再開時間Ｔｒのカウントダウンが０になるまで待機する状態など、様々な待機状態となっている。この待機状態中に再び移動端末２１からＢＵを受信した場合には、図５に示すフローチャートに示す処理を繰り返す一方、認証サーバ３２から認証結果を受信した場合や仮Binding時間Ｔ１、Binding時間Ｔ２、認証要求有効時間Ｔａ、認証要求再開時間Ｔｒのカウントダウンが０に

なった場合には、図７に示すフローチャートの処理を行う。

図７は、本発明の第２の実施の形態における認証サーバから認証結果を受信した場合及び所定の時間が経過した場合のＭＡＰの処理の詳細を示すフローチャートである。なお、図７に示すフローチャートは、図５に示すフローチャートから連続したものであり、図５に示す待機状態（ステップＳ３３３）と図７に示す待機状態（ステップＳ３３３）は同一ステップである。

まず、ＭＡＰ１０が、認証サーバ３２から移動端末２１の認証結果を受信（ステップＳ３４１）した場合、状態テーブル１９中にその認証処理の対象となった移動端末２１が存在しているか否か（当該移動端末２１に係るエントリが存在しているか否か）を調べる（ステップＳ３４２）。当該移動端末２１が存在していない場合には、すでにその移動端末２１に係る認証処理を行う必要はなく、再び待機状態に戻る。一方、当該移動端末２１が存在する場合には、認証結果が許可を示すものか否かを判定する（ステップＳ３４３）。

認証結果が許可を示すものであった場合には、ＭＡＰ１０は、状態テーブル１９中の当該移動端末２１の認証結果を「認証成功」に設定し（ステップＳ３４４）、認証成功の場合の処理（ステップＳ３１７～Ｓ３１９までの処理と同一）を行う（ステップＳ３４５）一方、認証結果が不許可を示すものであった場合には、ＭＡＰ１０は、状態テーブル１９中の当該移動端末２１の認証結果を「認証失敗」に設定し（ステップＳ３４６）、認証失敗の場合の処理（ステップＳ３２０～Ｓ３２２までの処理と同一）を行って（ステップＳ３４７）、再び待機状態に戻る。

また、認証要求再開時間Ｔｒが０になった（ステップＳ３４８）場合には、その移動端末２１に対する接続禁止区間の設定を終了し、状態テーブル１９中から、その移動端末２１に係るエントリを削除する（ステ

ップＳ３４９）。また、認証要求有効時間Ｔａが０になった（ステップＳ３５０）場合には、認証サーバ３２から認証結果を取得することができず、状態テーブル１９中の当該移動端末２１の認証結果を「認証失敗」に設定し（ステップＳ３５１）、認証失敗の場合の処理（ステップＳ３２０～Ｓ３２２までの処理と同一）を行って（ステップＳ３５２）、再び待機状態に戻る。

また、仮Binding時間Ｔ１又はBinding時間Ｔ２が０になった（ステップＳ３５３）場合には、その移動端末２１に提供している接続サービスの有効期限が切れて無効になったとみなし、ＲＣｏＡ／ＬＣｏＡテーブルから当該移動端末２１に関する情報を削除して(ステップＳ３５４)、再び待機状態に戻る。

以上、説明したように、本発明の第２の実施の形態によれば、シームレスハンドオーバを目的とし、すでに標準化が進められているＨＭＩＰｖ６の位置登録シーケンス中に認証シーケンスを含め、さらに、認証シーケンスに時間がかかる場合を考慮して、その認証時間中においても、移動端末２１がネットワークにアクセスできるようにすることによって、ＩＰアドレスの移動に係る制御と同時に認証処理を行うことが可能となり、位置登録シーケンスと認証シーケンスが独立に行われていた場合や本発明の第１の実施の形態で説明した位置登録シーケンスと認証シーケンスとを同時に行う技術に比べて、さらに、ハンドオーバに要する時間が短縮し、移動端末２１に対してシームレスな接続サービスを提供することが可能となる。

また、上記の第２の実施の形態では、特にＨＭＩＰｖ６を利用する無線通信システムを例にして説明したが、下記の１～４に示す

１．短時間だけ仮の接続許可を与えること（上記の仮Binding時間Ｔ１に対応）

２．接続許可に時間制限を設けること（上記のBinding時間Ｔ２に対応）

３．認証サーバに認証要求を行う際にその応答を受けるまでの時間を設定すること（上記の認証要求有効時間Ｔａに対応）

４．認証に失敗した移動端末に対しては、一定時間だけ接続を禁止すること（上記の認証要求再開時間Ｔｒに対応）

は、ＨＭＩＰｖ６に限らず、例えば、グローバルＩＰｖ４や、従来の技術で説明したDiameter Mobile IPv4など、他の通信プロトコルを利用する無線通信システムにおいても適用可能である。

この場合、上記の第２の実施の形態において、ＭＡＰ１０を管理サーバ、Binding Updateを接続要求、Binding Acknowledgementを接続要求への応答、Binding時間を接続許可時間、ＬＣｏＡを端末識別情報、ＲＣｏＡ／ＬＣｏＡテーブルを接続許可テーブルなどとそれぞれ読み換え、状態テーブルとして、図８に示す状態テーブルを用いることにより、HMIPv6以外の通信プロトコルへの一般化が可能である。また、上記の第２の実施の形態では、管理サーバが、認証に成功した移動端末２１に対して、すぐに接続サービスを提供するようにしているが、移動端末２１からの接続要求があってその認証に成功した場合、まず、状態テーブルに「認証成功」の旨を記載しておき、次に、再び当該移動端末から接続要求を受信した場合に、状態テーブルの「認証成功」の記載を確認して、初めて通常の時間の接続サービスを提供することも可能である。

産業上の利用可能性

以上、説明したように、本発明によれば、ＨＭＩＰｖ６を用いて移動端末のリンク接続を管理する無線通信システムにおける無線通信管理方法に関し、移動端末のリンク接続を管理するサーバに対して、移動端末

が、リンク接続を変更するための情報と同時に、所望のネットワークにアクセスするための認証に係る情報を送信し、位置登録シーケンスと認証シーケンスとを同時に行えるようにしているので、移動端末がリンク接続を変更するハンドオーバ時に、スムーズにハンドオーバを行えるようにするとともに、リンク接続の変更に要する時間を短縮することが可能となる。

請 求 の 範 囲

1. ＨＭＩＰｖ６を用いて移動端末のリンク接続を管理する無線通信システムにおける無線通信管理方法であって、

前記移動端末の前記リンク接続を管理するサーバに対して、前記移動端末が、前記リンク接続を変更するための情報と同時に、所望のネットワークにアクセスするための認証に係る情報を送信し、前記移動端末の前記リンク接続の変更に要する時間を短縮する無線通信管理方法。

2. 前記移動端末が、前記リンク接続を変更するための情報と、前記認証に係る情報とを１つの情報として送信し、前記リンク接続を管理するサーバが、前記１つの情報から、前記リンク接続を変更するための情報及び前記認証に係る情報のそれぞれを取得する請求項１に記載の無線通信管理方法。

3. 前記リンク接続を管理するサーバが、前記認証に係る情報を用いた認証処理による認証結果を取得する請求項１に記載の無線通信管理方法。

4. 前記リンク接続を管理するサーバが、前記移動端末の認証を行う認証サーバとの通信を行い、前記認証結果を取得する請求項３に記載の無線通信管理方法。

5. 前記移動端末の前記リンク接続の変更を確認した旨を通知する情報と、前記認証結果とを１つの情報として、前記移動端末に送信する請求項３に記載の無線通信管理方法。

6. 前記リンク接続を管理するサーバが、前記移動端末の前記リンク接続の変更を確認した旨を通知する情報を前記移動端末に送信し、その後、前記認証結果を取得できた場合に前記認証結果を前記移動端末に送信する請求項3に記載の無線通信管理方法。

7. 前記リンク接続を管理するサーバが、前記認証結果の取得までの時間を設定し、前記認証結果の取得までの時間内に前記認証結果を取得できた場合、次に前記移動端末から前記リンク接続を変更するための情報を受信した際に、前記移動端末の前記リンク接続の変更を確認した旨を通知する情報と共に、前記認証結果を前記移動端末に送信する請求項6に記載の無線通信管理方法。

8. 前記リンク接続を管理するサーバが、前記移動端末が前記所望のネットワークへのアクセスを仮許可する所定の仮許可時間を設定し、前記移動端末の前記リンク接続の変更を確認した旨を通知する情報と共に、前記所定の時間だけ前記所望のネットワークへのアクセスの許可を通知する情報を前記移動端末に送信する請求項7に記載の無線通信管理方法。

9. 前記リンク接続を管理するサーバが、前記所定の仮許可時間よりも長い時間であって、前記移動端末が前記所望のネットワークへのアクセスを許可する所定の許可時間を設定し、前記認証結果が認証成功であった場合、前記移動端末の前記リンク接続の変更を確認した旨を通知する情報と共に、所定の許可時間だけ前記所望のネットワークへのアクセスの許可を通知する情報を前記移動端末に送信する請求項8に記載の無線通信管理方法。

１０．　前記リンク接続を管理するサーバが、前記所定の仮許可時間又は前記所定の許可時間だけ前記所望のネットワークへのアクセスを許可した前記移動端末の前記リンク接続の変更に係る登録を行い、前記所定の仮許可時間又は前記所定の許可時間が経過した場合、前記移動端末の前記リンク接続の変更に係る登録を削除する請求項８に記載の無線通信管理方法。

１１．　前記リンク接続を管理するサーバが、前記認証結果の取得までの時間を設定し、前記認証結果の取得までの時間内に前記認証結果を取得できなかった場合、前記認証結果を認証失敗とする請求項３に記載の無線通信管理方法。

１２．　前記リンク接続を管理するサーバが、前記移動端末に対して所定の接続禁止時間を設定し、前記移動端末に対して前記認証結果として認証失敗を通知した場合には、前記認証失敗の通知から前記所定の接続禁止時間だけ、前記認証失敗であった前記移動端末の前記リンク接続の変更に係る処理及び前記認証に係る処理を行わないようにする請求項５又は６に記載の無線通信管理方法。

１３．　前記リンク接続を管理するサーバが、前記移動端末に対して前記認証結果として認証成功を通知した場合のみ、前記認証成功であった前記移動端末の前記リンク接続の変更に係る登録を行うようにする請求項５又は６に記載の無線通信管理方法。

１４．　移動端末のリンク接続を管理する無線通信システムにおける無線通信管理方法であって、

前記移動端末の前記リンク接続を管理するサーバに対して、前記移動端末が、前記リンク接続を変更するための情報と同時に、所望のネットワークにアクセスするための認証に係る情報を送信し、

前記リンク接続を管理するサーバが、前記認証に係る情報を用いた認証処理による認証結果の取得までの時間を設定し、前記認証結果の取得までの時間内に前記認証結果を取得できた場合、前記認証結果を前記移動端末に送信する無線通信管理方法。

１５．　前記リンク接続を管理するサーバが、前記移動端末が前記所望のネットワークへのアクセスを仮許可する所定の仮許可時間を設定し、前記所定の時間だけ前記所望のネットワークへのアクセスの許可を通知する情報を前記移動端末に送信する請求項１４に記載の無線通信管理方法。

１６．　前記リンク接続を管理するサーバが、前記所定の仮許可時間よりも長い時間であって、前記移動端末が前記所望のネットワークへのアクセスを許可する所定の許可時間を設定し、前記認証結果が認証成功であった場合、所定の許可時間だけ前記所望のネットワークへのアクセスの許可を通知する情報を前記移動端末に送信する請求項１５に記載の無線通信管理方法。

１７．　前記所定の仮許可時間又は前記所定の許可時間が経過した場合、前記リンク接続を管理するサーバは、前記移動端末の前記接続を切断する請求項１５又は１６に記載の無線通信管理方法。

１８．　移動端末のリンク接続を管理する無線通信システムにおける

無線通信管理方法であって、

前記移動端末の前記リンク接続を管理するサーバに対して、前記移動端末が、前記リンク接続を変更するための情報と同時に、所望のネットワークにアクセスするための認証に係る情報を送信し、

前記リンク接続を管理するサーバが、前記認証に係る情報を用いた認証処理による認証結果の取得までの時間を設定し、前記認証結果の取得までの時間内に前記認証結果を取得できなかった場合、前記認証結果を認証失敗とする無線通信管理方法。

１９．　前記リンク接続を管理するサーバが、前記移動端末に対して所定の接続禁止時間を設定し、前記移動端末に対して前記認証結果として認証失敗を通知した場合には、前記認証失敗の通知から前記所定の接続禁止時間だけ、前記認証失敗であった前記移動端末に係る処理を行わないようにする請求項１４又は１８に記載の無線通信管理方法。

２０．　前記リンク接続を管理するサーバが、前記移動端末に対して前記認証結果として認証成功を通知した場合のみ、前記認証成功であった前記移動端末の前記リンク接続の変更に係る登録を行うようにする請求項１４に記載の無線通信管理方法。

２１．　ＨＭＩＰｖ６を用いて移動端末のリンク接続を管理する無線通信管理サーバであって、

前記移動端末から、前記リンク接続を変更するための情報と所望のネットワークにアクセスするための認証に係る情報とを１つの情報で受信し、前記１つの情報から、前記リンク接続を変更するための情報及び前記認証に係る情報のそれぞれを取得するよう構成されている無線通信管

理サーバ。

２２．　前記認証に係る情報を用いた認証処理による認証結果を取得するよう構成されている請求項２１に記載の無線通信管理サーバ。

２３．　前記移動端末の認証を行う認証サーバとの通信を行う手段を有し、

前記認証結果を取得するよう構成されている請求項２２に記載の無線通信管理サーバ。

２４．　前記移動端末の前記リンク接続の変更を確認した旨を通知する情報と前記認証結果とを１つの情報として、前記移動端末に送信するよう構成されている請求項２２に記載の無線通信管理サーバ。

２５．　前記移動端末の前記リンク接続の変更を確認した旨を通知する情報を前記移動端末に送信し、その後、前記認証結果を取得できた場合に前記認証結果を前記移動端末に送信するよう構成されている請求項２２に記載の無線通信管理サーバ。

２６．　前記認証結果の取得までの時間を設定する時間設定手段を有し、前記認証結果の取得までの時間内に前記認証結果を取得できた場合、次に前記移動端末から前記リンク接続を変更するための情報を受信した際に、前記移動端末の前記リンク接続の変更を確認した旨を通知する情報と共に、前記認証結果を前記移動端末に送信するよう構成されている請求項２５に記載の無線通信管理サーバ。

２７．　前記移動端末に対して前記所望のネットワークへのアクセスを仮許可する所定の仮許可時間を設定する時間設定手段を有し、

前記移動端末の前記リンク接続の変更を確認した旨を通知する情報と共に、前記所定の時間だけ前記所望のネットワークへのアクセスの許可を通知する情報を前記移動端末に送信するよう構成されている請求項２６に記載の無線通信管理サーバ。

２８．　前記移動端末に対して、前記所定の仮許可時間よりも長い時間であって、前記移動端末が前記所望のネットワークへのアクセスを許可する所定の許可時間を設定する時間設定手段を有し、

前記認証結果が認証成功であった場合、前記移動端末の前記リンク接続の変更を確認した旨を通知する情報と共に、所定の許可時間だけ前記所望のネットワークへのアクセスの許可を通知する情報を前記移動端末に送信するよう構成されている請求項２７に記載の無線通信管理サーバ。

２９．　前記所定の仮許可時間又は前記所定の許可時間だけ前記所望のネットワークへのアクセスを許可した前記移動端末の前記リンク接続の変更に係る登録を行う情報登録手段と、

前記所定の仮許可時間又は前記所定の許可時間が経過した場合、前記移動端末の前記リンク接続の変更に係る登録を削除する情報削除手段とを、

有する請求項２７に記載の無線通信管理サーバ。

３０．　前記認証結果の取得までの時間を設定する時間設定手段と、

前記認証結果の取得までの時間内に前記認証結果を取得できなかった場合、前記認証結果を認証失敗とする判定手段とを、

有する請求項２２に記載の無線通信管理サーバ。

３１．　前記移動端末に対して所定の接続禁止時間を設定する時間設定手段と、

前記移動端末に対して前記認証結果として認証失敗を通知した場合には、前記認証失敗の通知から前記所定の接続禁止時間だけ、前記認証失敗であった前記移動端末の前記リンク接続の変更に係る処理及び前記認証に係る処理を行わないよう制御する制御手段とを、

有する請求項２４又は２５に記載の無線通信管理サーバ。

３２．　前記移動端末に対して前記認証結果として認証成功を通知した場合のみ、前記認証成功であった前記移動端末の前記リンク接続の変更に係る登録を行うよう制御する制御手段を有する請求項２４又は２５に記載の無線通信管理サーバ。

３３．　移動端末のリンク接続を管理する無線通信管理サーバであって、

前記移動端末から、前記リンク接続を変更するための情報と同時に、所望のネットワークにアクセスするための認証に係る情報を受信する受信手段と、

前記認証に係る情報を用いた認証処理による認証結果の取得までの時間を設定する時間設定手段と、

前記認証結果の取得までの時間内に前記認証結果を取得できた場合、前記認証結果を前記移動端末に送信する送信手段とを、

有する無線通信管理サーバ。

３４．　前記移動端末が前記所望のネットワークへのアクセスを仮許可する所定の仮許可時間を設定する時間設定手段を有し、

前記所定の時間だけ前記所望のネットワークへのアクセスの許可を通知する情報を前記移動端末に送信するよう構成されている請求項３３に記載の無線通信管理サーバ。

３５．　前記所定の仮許可時間よりも長い時間であって、前記移動端末が前記所望のネットワークへのアクセスを許可する所定の許可時間を設定する時間設定手段を有し、

前記認証結果が認証成功であった場合、所定の許可時間だけ前記所望のネットワークへのアクセスの許可を通知する情報を前記移動端末に送信するよう構成されている請求項３４に記載の無線通信管理サーバ。

３６．　前記所定の仮許可時間又は前記所定の許可時間が経過した場合、前記移動端末の前記接続を切断する制御手段を有する請求項３４又は３５に記載の無線通信管理サーバ。

３７．　移動端末のリンク接続を管理する無線通信システムにおける無線通信管理サーバであって、

前記移動端末から、前記リンク接続を変更するための情報と同時に、所望のネットワークにアクセスするための認証に係る情報を受信する受信手段と、

前記リンク接続を管理するサーバが、前記認証に係る情報を用いた認証処理による認証結果の取得までの時間を設定する時間設定手段と、

前記認証結果の取得までの時間内に前記認証結果を取得できなかった場合、前記認証結果を認証失敗として、前記認証結果を前記移動端末に

送信する送信手段とを、

有する無線通信管理サーバ。

３８．　前記移動端末に対して所定の接続禁止時間を設定する時間設定手段と、

前記移動端末に対して前記認証結果として認証失敗を通知した場合には、前記認証失敗の通知から前記所定の接続禁止時間だけ、前記認証失敗であった前記移動端末に係る処理を行わないよう制御する制御手段とを、

有する請求項３３又は３７に記載の無線通信管理サーバ。

３９．　前記移動端末に対して前記認証結果として認証成功を通知した場合のみ、前記認証成功であった前記移動端末の前記リンク接続の変更に係る登録を行うよう制御する制御手段を有する請求項３３に記載の無線通信管理サーバ。

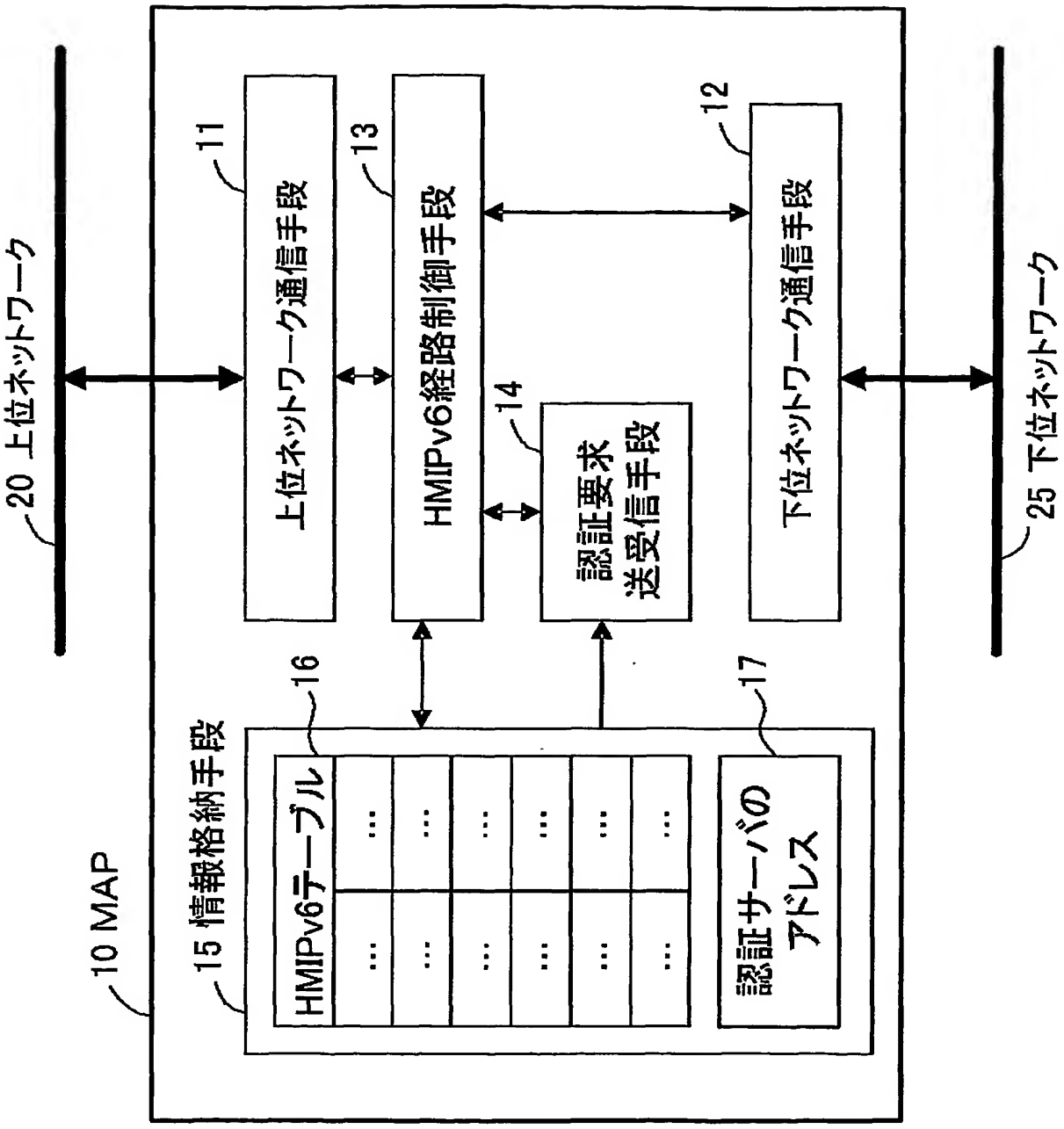

20 上位ネットワーク
11
上位ネットワーク通信手段
13
HMIPv6経路制御手段
12
下位ネットワーク通信手段
25 下位ネットワーク
14
認証要求
送受信手段
10 MAP
15 情報格納手段
16
HMIPv6テーブル
17
認証サーバの
アドレス

FIG. 1

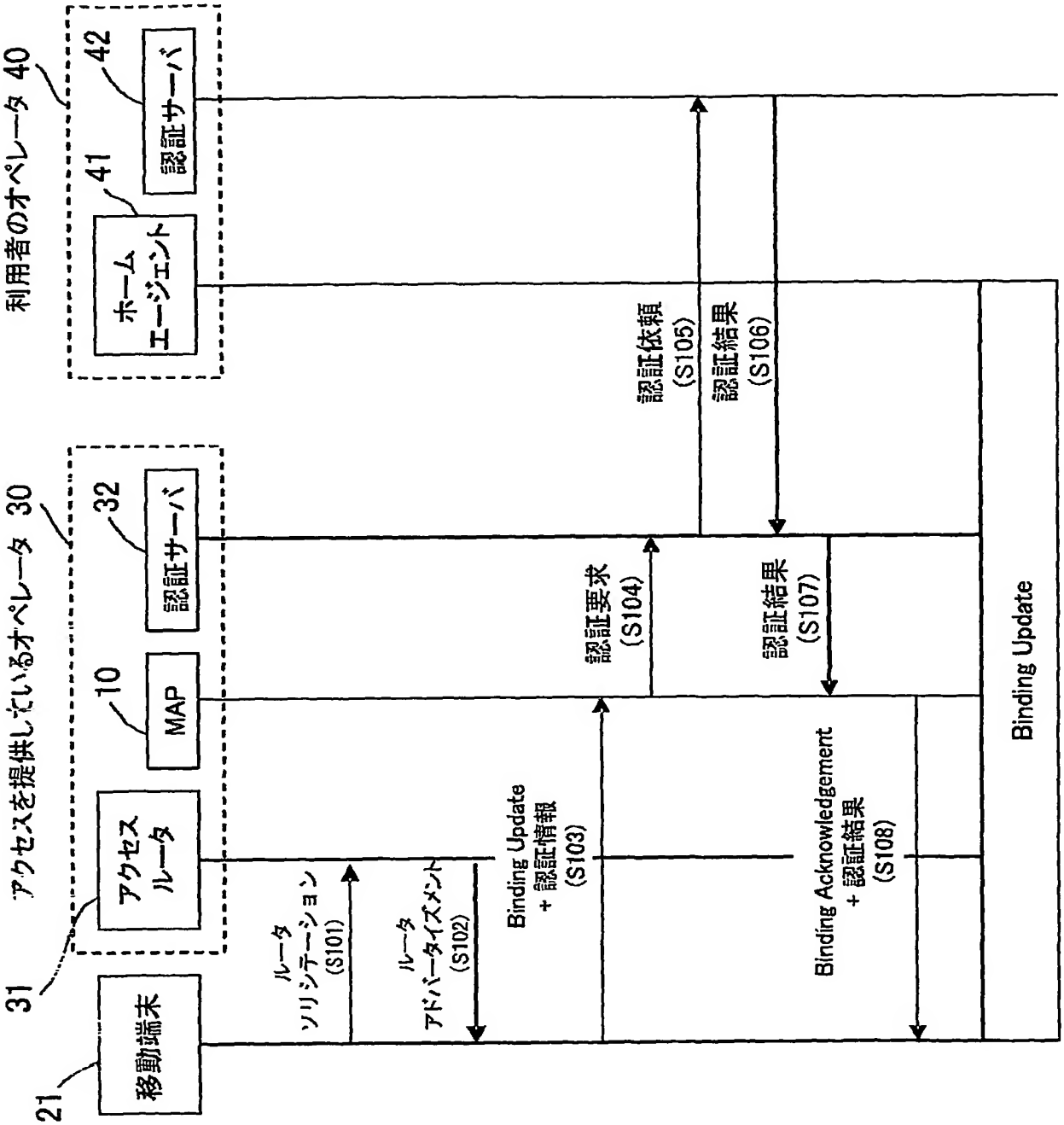

利用者のオペレータ 40
ホーム エージェント
41
認証サーバ
42
アクセスを提供しているオペレータ 30
31
アクセス ルータ
MAP
10
認証サーバ
32
移動端末
21
ルータ ソリシテーション (S101)
ルータ アドバータイズメント (S102)
Binding Update + 認証情報 (S103)
認証要求 (S104)
認証依頼 (S105)
認証結果 (S106)
認証結果 (S107)
Binding Acknowledgement + 認証結果 (S108)
Binding Update

FIG. 2

FIG. 3

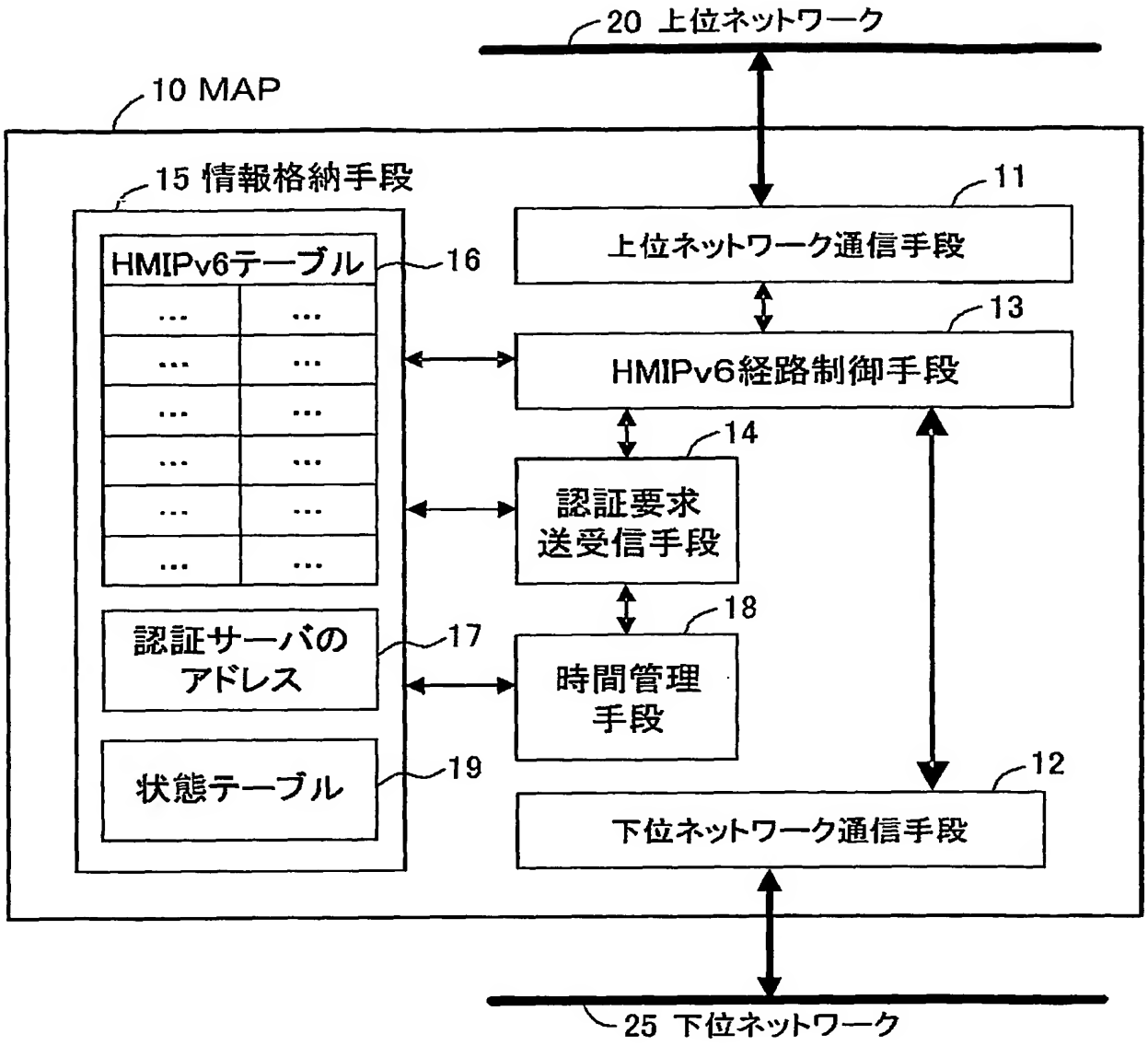

20 上位ネットワーク
10 MAP
15 情報格納手段
HMIPv6テーブル
16
11
上位ネットワーク通信手段
13
HMIPv6経路制御手段
14
認証要求
送受信手段
18
時間管理
手段
認証サーバの
アドレス
17
状態テーブル
19
12
下位ネットワーク通信手段
25 下位ネットワーク

FIG. 4

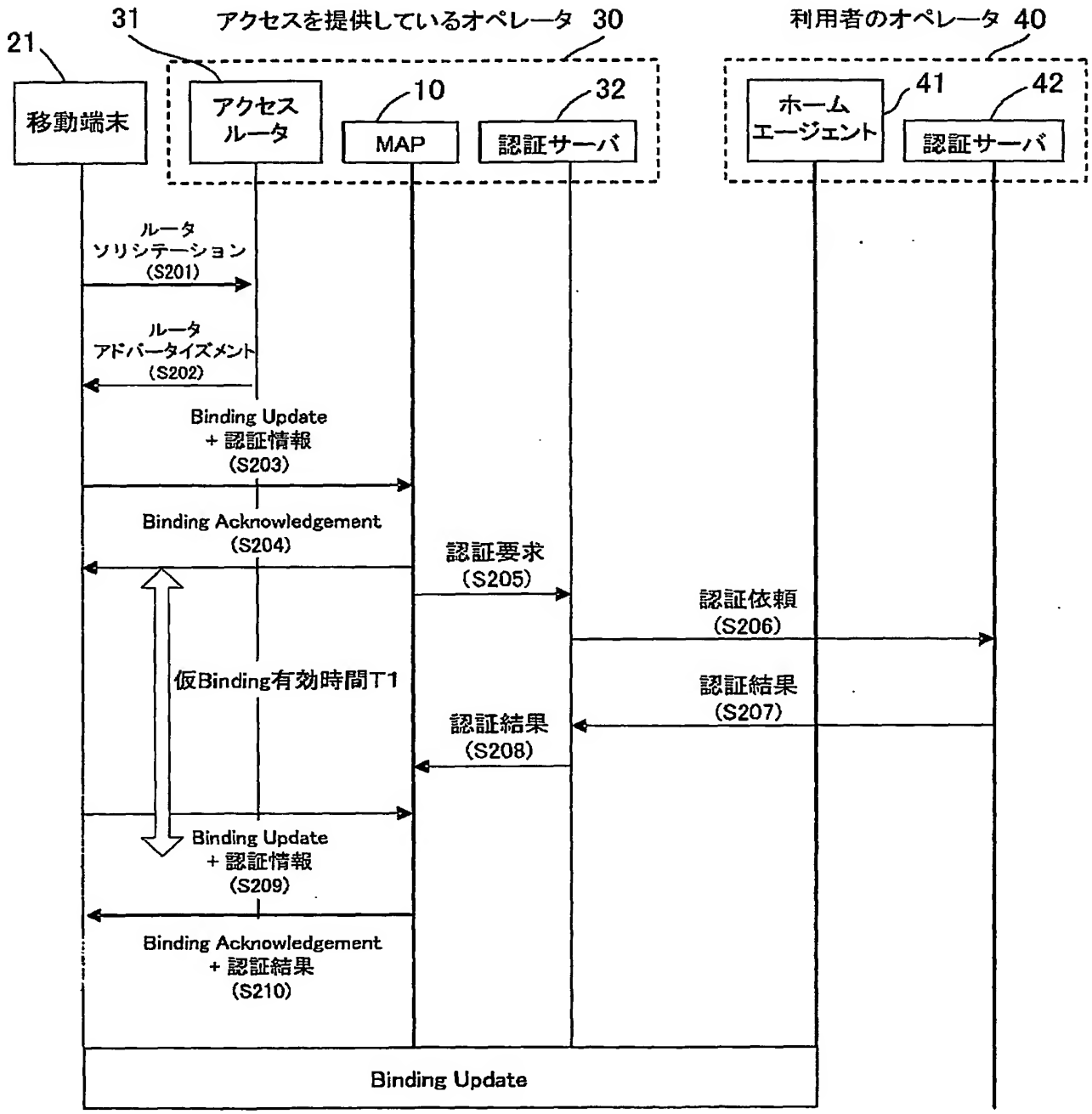

21
31
アクセスを提供しているオペレータ 30
利用者のオペレータ 40
移動端末
アクセス ルータ
10
MAP
32
認証サーバ
ホーム エージェント
41
42
認証サーバ
ルータ ソリシテーション (S201)
ルータ アドバータイズメント (S202)
Binding Update + 認証情報 (S203)
Binding Acknowledgement (S204)
認証要求 (S205)
認証依頼 (S206)
仮Binding有効時間T1
認証結果 (S207)
認証結果 (S208)
Binding Update + 認証情報 (S209)
Binding Acknowledgement + 認証結果 (S210)
Binding Update

FIG. 5

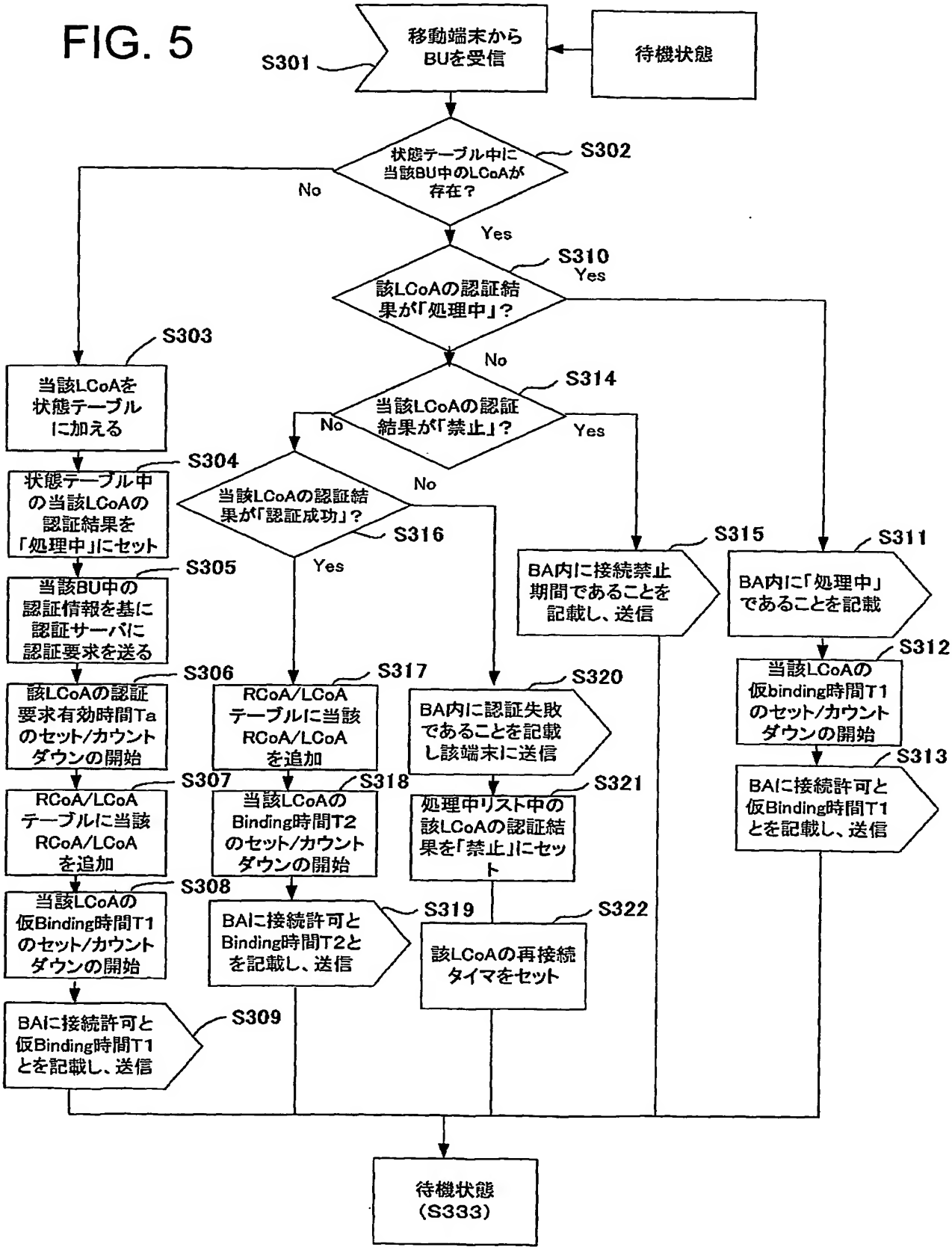

S301
移動端末から BUを受信
待機状態
状態テーブル中に 当該BU中のLCoAが 存在？
S302
No
Yes
該LCoAの認証結 果が「処理中」？
S310
Yes
No
当該LCoAの認証 結果が「禁止」？
S314
No
Yes
当該LCoAの認証結 果が「認証成功」？
No
S316
Yes
S303
当該LCoAを 状態テーブル に加える
S304
状態テーブル中 の当該LCoAの 認証結果を 「処理中」にセット
S305
当該BU中の 認証情報を基に 認証サーバに 認証要求を送る
S306
該LCoAの認証 要求有効時間Ta のセット/カウント ダウンの開始
S307
RCoA/LCoA テーブルに当該 RCoA/LCoA を追加
S308
当該LCoAの 仮Binding時間T1 のセット/カウント ダウンの開始
BAに接続許可と 仮Binding時間T1 とを記載し、送信
S309
S317
RCoA/LCoA テーブルに当該 RCoA/LCoA を追加
S318
当該LCoAの Binding時間T2 のセット/カウント ダウンの開始
S319
BAに接続許可と Binding時間T2と を記載し、送信
S320
BA内に認証失敗 であることを記載 し該端末に送信
S321
処理中リスト中の 該LCoAの認証結 果を「禁止」にセッ ト
S322
該LCoAの再接続 タイマをセット
S315
BA内に接続禁止 期間であることを 記載し、送信
S311
BA内に「処理中」 であることを記載
S312
当該LCoAの 仮binding時間T1 のセット/カウント ダウンの開始
S313
BAに接続許可と 仮Binding時間T1 とを記載し、送信
待機状態 (S333)

FIG. 6

端末の LCoA	認証結果	認証要求有効時間 Ta	認証要求再開時間 Tr	仮Binding時間T1 Binding時間T2
2002 : : ID101	処理中	87	—	45
2002 : : ID11	認証失敗	—	1532	—
2002 : : ID334	認証成功	—	—	231003
...	...	...	...	...

FIG. 7

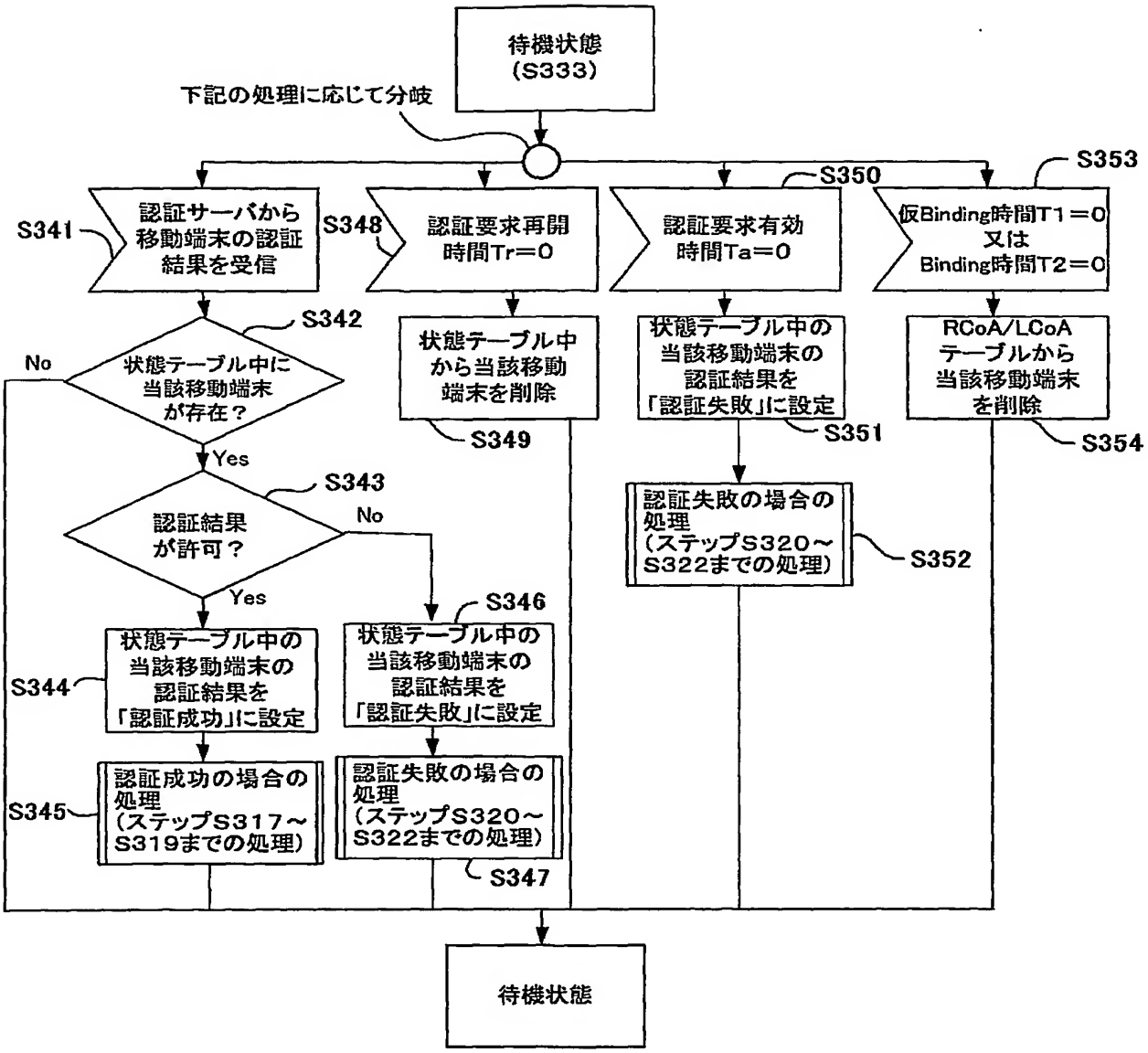

待機状態
(S333)
下記の処理に応じて分岐
S341
認証サーバから移動端末の認証結果を受信
S342
状態テーブル中に当該移動端末が存在？
No
Yes
S343
認証結果が許可？
No
Yes
S344
状態テーブル中の当該移動端末の認証結果を「認証成功」に設定
S345
認証成功の場合の処理（ステップS317～S319までの処理）
S346
状態テーブル中の当該移動端末の認証結果を「認証失敗」に設定
認証失敗の場合の処理（ステップS320～S322までの処理）
S347
S348
認証要求再開時間Tr＝0
S349
状態テーブル中から当該移動端末を削除
S350
認証要求有効時間Ta＝0
S351
状態テーブル中の当該移動端末の認証結果を「認証失敗」に設定
認証失敗の場合の処理（ステップS320～S322までの処理）
S352
S353
仮Binding時間T1＝0又はBinding時間T2＝0
S354
RCoA/LCoAテーブルから当該移動端末を削除
待機状態

FIG. 8

端末ID	認証結果	認証要求有効時間 Ta	認証要求再開時間 Tr	仮Binding時間T1 Binding時間T2
MT101	処理中	87	—	45
MT11	認証失敗	—	1532	—
MT334	認証成功	—	—	231003
...	...	...	...	...

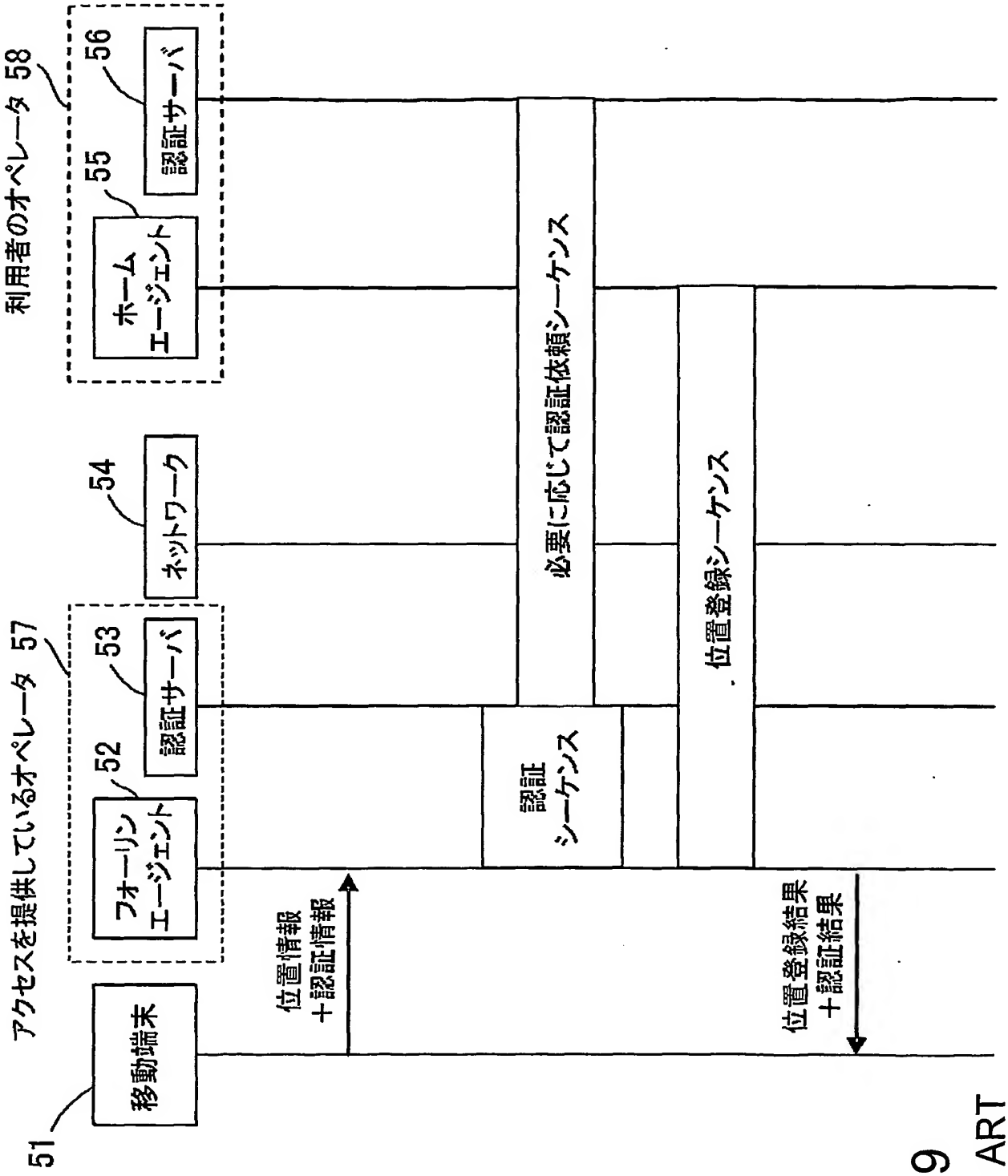


FIG. 9
PRIOR ART

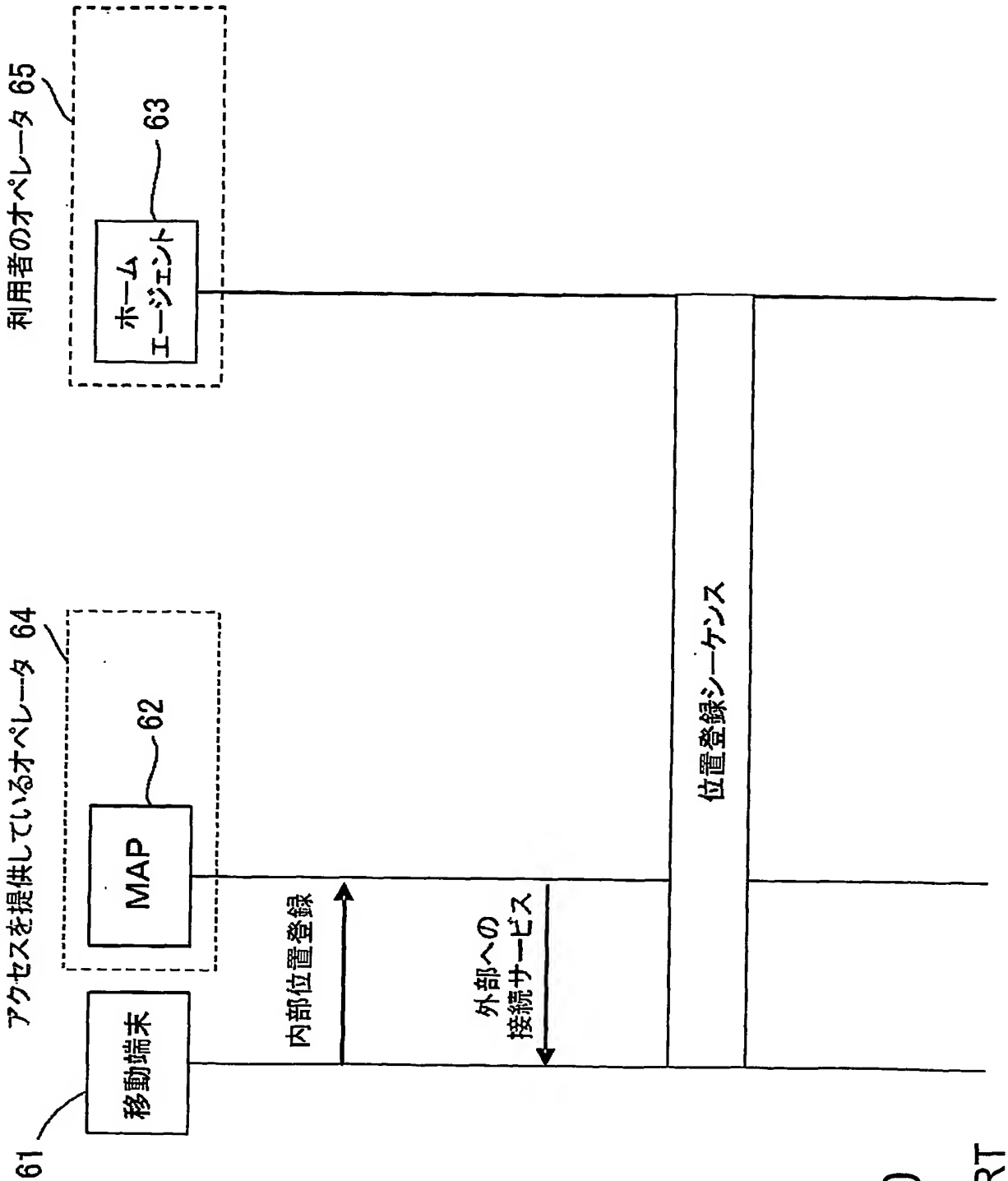


FIG. 10
PRIOR ART

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP03/13624

A. CLASSIFICATION OF SUBJECT MATTER
Int.Cl[7] H04Q7/38, H04L12/56

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
Int.Cl[7] H04Q7/00-7/38, H04L12/56

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Jitsuyo Shinan Koho	1922-1996	Toroku Jitsuyo Shinan Koho	1994-2004
Kokai Jitsuyo Shinan Koho	1971-2004	Jitsuyo Shinan Toroku Koho	1996-2004

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	JP 2002-185520 A (Fujitsu Ltd.), 28 June, 2002 (28.06.02), Fig. 11; Par. Nos. [0035] to [0053] & US 2002/0071417 A1	1-7,11-14, 18-26,30-33, 37-39
Y	WO 01/067798 A (TELEFONAKTIEBOLAGET ERICSSON LM(publ)), 13 September, 2001 (13.09.01),	1-7,11-14, 18-26,30-33, 37-39
A	Full text & JP 2003-526297 W & EP 1260113 A1 & AU 200136319 A & US 2001/0046223 A1	8-10,15-17, 27-29,34-36
A	JP 2002-271376 A (Sony Corp.), 20 September, 2002 (20.09.02), Full text & US 2002/00172207 A1	1-39

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier document but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search 09 February, 2004 (09.02.04)	Date of mailing of the international search report 24 February, 2004 (24.02.04)
Name and mailing address of the ISA/ Japanese Patent Office Facsimile No.	Authorized officer Telephone No.

Form PCT/ISA/210 (second sheet) (July 1998)

国際調[redacted]告　　国際出願番[redacted]PCT／JP03／13624

A.　発明の属する分野の分類（国際特許分類（IPC））
Int. Cl⁷ H04Q 7／38
Int. Cl⁷ H04L12／56

B.　調査を行った分野

調査を行った最小限資料（国際特許分類（IPC））
Int. Cl⁷ H04Q 7／00 － 7／38
Int. Cl⁷ H04L12／56

最小限資料以外の資料で調査を行った分野に含まれるもの
日本国実用新案公報　1922－1996年
日本国公開実用新案公報　1971－2004年
日本国登録実用新案公報　1994－2004年
日本国実用新案登録公報　1996－2004年

国際調査で使用した電子データベース（データベースの名称、調査に使用した用語）

C.　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
Y	JP 2002－185520 A（富士通株式会社） 2002.06.28，図11、第35－53段落 &US 2002／0071417 A1	1-7, 11-14, 18-26, 30-33, 37-39
Y	WO 01／067798 A (TELEFONAKTIEBOLAGET ERICSSON LM(publ)) 2001.09.13，全文 &JP 2003－526297 W	1-7, 11-14, 18-26, 30-33, 37-39
A	&EP 1260113 A1 &AU 200136319 A &US 2001／0046223 A1	8-10, 15-17, 27-29, 34-36

☒ C欄の続きにも文献が列挙されている。　☐ パテントファミリーに関する別紙を参照。

＊ 引用文献のカテゴリー
「A」特に関連のある文献ではなく、一般的技術水準を示すもの
「E」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの
「L」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）
「O」口頭による開示、使用、展示等に言及する文献
「P」国際出願日前で、かつ優先権の主張の基礎となる出願の日の後に公表された文献
「T」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの
「X」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの
「Y」特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの
「&」同一パテントファミリー文献

国際調査を完了した日	国際調査報告の発送日
09.02.2004	24.2.2004

国際調査機関の名称及びあて先	特許庁審査官（権限のある職員）	
日本国特許庁（ISA／JP） 郵便番号100－8915 東京都千代田区霞が関三丁目4番3号	青木 健　印	5J　9571
	電話番号　03－3581－1101　内線　3534	

様式PCT／ISA／210（第2ページ）（1998年7月）

C（続き）．　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
A	JP　2002－271376　A（ソニー株式会社） 2002．09．20，全文 &US　2002／00172207　A1	1-39